Kaspersky Total Security



دليل المستخدم

إصدار التطبيق: 15.0

مدونة السندباد

www.Al-Sindbad.net


KASPERSKY lab

جدول المحتويات

حول هذا الدليل

هذا المستند هو دليل مستخدم Kaspersky Total Security.

لاستخدام Kaspersky Total Security بشكل سليم، ينبغي أن تتعرف على واجهة نظام التشغيل الذي تستخدمه، وأن تكون لديك خبرة مع الأساليب الأساسية الخاصة بهذا النظام، إلى جانب معرفة كيفية العمل مع البريد الإلكتروني والإنترنت.

فيما يلي يتم توضيح الغرض من هذا الدليل:

- كيفية تثبيت Kaspersky Total Security، وتفعيله، واستخدامه.
- توفير طريقة للعثور سريعًا على معلومات حول المشكلات المتعلقة بتطبيق Kaspersky Total Security.
- شرح مصادر المعلومات الأخرى المتعلقة بالتطبيق وطرق تلقي الدعم الفني.

في هذا القسم

في هذا الدليل

يحتوي هذا المستند على الأقسام التالية:

مصادر المعلومات المتعلقة بالتطبيق

يصف هذا القسم مصادر المعلومات المتعلقة بالتطبيق ويسرد مواقع الويب التي يمكنك استخدامها لمناقشة استخدام التطبيق.

Kaspersky Total Security

يصف هذا القسم مزايا التطبيق ويقدم معلومات موجزة حول وظائف التطبيق ومكوناته. ستتعرف على العناصر المضمنة في حزمة التوزيع والخدمات المتوفرة للمستخدمين المسجلين للتطبيق. يوفر هذا القسم معلومات حول متطلبات البرامج والأجهزة التي يجب أن يفي بها الكمبيوتر حتى يتمكن المستخدم من تثبيت التطبيق عليه.

تثبيت التطبيق وإزالته

يحتوي هذا القسم على إرشادات خطوة بخطوة لتثبيت التطبيق وإزالته.

ترخيص التطبيق

يوفر هذا القسم معلومات حول البنود الأساسية المتعلقة بتفعيل التطبيق. اقرأ هذا القسم لتتعرف على المزيد حول الهدف من "اتفاقية ترخيص المستخدم النهائي"، وطرق تفعيل التطبيق، وتجديد الترخيص.

إدارة إخطارات التطبيق

يوفر هذا القسم معلومات حول كيفية إدارة إخطارات التطبيق.

تقييم حالة حماية الكمبيوتر وحل مشكلات الأمان

يقدم هذا القسم معلومات حول كيفية تقييم حالة أمان الكمبيوتر وإصلاح التهديدات الأمنية.

تحديث قواعد البيانات والوحدات البرمجية

يحتوي هذا القسم على تعليمات خطوة بخطوة حول كيفية تحديث قواعد البيانات ووحدات برامج التطبيق.

فحص الكمبيوتر

يحتوي هذا القسم على تعليمات خطوة بخطوة حول كيفية فحص الكمبيوتر لاكتشاف الفيروسات والبرامج الخبيثة والثغرات الأمنية.

استكشاف أخطاء نظام التشغيل وإصلاحها بعد الإصابة

يقدم هذا القسم معلومات حول كيفية استعادة نظام التشغيل بعد إصابته بالفيروسات.

حماية البريد الإلكتروني

يقدم هذا القسم معلومات حول كيفية حماية البريد الإلكتروني من البريد الإلكتروني غير المرغوب فيه لاكتشاف الفيروسات والتهديدات الأخرى.

حماية البيانات الخاصة على الإنترنت

يوفر هذا القسم معلومات حول كيفية جعل استعراض الإنترنت آمنًا وحماية بياناتك من السرقة.

إزالة تتبعات النشاط على الكمبيوتر والإنترنت

يوفر هذا القسم معلومات حول كيفية مسح تتبعات نشاط المستخدم من الكمبيوتر.

التحكم في أنشطة المستخدمين الموجودة على الكمبيوتر والإنترنت

يقدم هذا القسم معلومات حول كيفية التحكم في إجراءات المستخدمين على الكمبيوتر والإنترنت باستخدام Kaspersky Total Security.

إدارة حماية الكمبيوتر عن بُعد

يوضح هذا القسم كيفية إدارة حماية الكمبيوتر عن بُعد بواسطة مدخل My Kaspersky.

الحفاظ على موارد نظام التشغيل لألعاب الكمبيوتر

يحتوي هذا القسم على تعليمات حول كيفية تحسين أداء نظام التشغيل لألعاب الكمبيوتر والتطبيقات الأخرى.

التعامل مع التطبيقات غير المعروفة

يوفر هذا القسم معلومات حول كيفية منع التطبيقات من إجراء عمليات غير مسموح بها على الكمبيوتر.

وضع التطبيقات الموثوقة

يوفر هذا القسم معلومات حول وضع التطبيقات الموثوق بها.

أداة التخلص من الملفات

يوضح هذا القسم كيفية استخدام Kaspersky Total Security لحذف البيانات نهائيًا ومن ثم لا يتمكن المحتالون من استعادته.

النسخ الاحتياطي والاستعادة

يوضح هذا القسم كيف يمكنك نسخ البيانات احتياطيًا باستخدام Kaspersky Total Security.

تخزين البيانات في مخازن البيانات

يوضح هذا القسم كيف يمكنك حماية الملفات والمجلدات على الكمبيوتر الخاص بك باستخدام مخازن البيانات.

الوصول المحمي بكلمة مرور للتحكم في **Kaspersky Total Security**

يحتوي هذا القسم على تعليمات حول كيفية حماية إعدادات التطبيق باستخدام كلمة مرور.

إيقاف حماية الكمبيوتر واستعادتها

يحتوي هذا القسم على تعليمات خطوة بخطوة حول كيفية تمكين التطبيق وتعطيله.

استعادة إعدادات التطبيق الافتراضية.

يحتوي هذا القسم على تعليمات حول كيفية استعادة إعدادات التطبيق الافتراضية.

عرض تقرير تشغيل التطبيق

يحتوي هذا القسم على تعليمات حول كيفية عرض تقارير التطبيق.

تطبيق إعدادات التطبيق على كمبيوتر آخر

يوفر هذا القسم معلومات حول كيفية تصدير إعدادات التطبيق وتطبيقها على كمبيوتر آخر.

المشاركة في شبكة اتصال أمان **Kaspersky**

يوفر هذا القسم معلومات حول شبكة اتصال أمان Kaspersky وكيفية المشاركة في KSN.

استخدام التطبيق من موجه الأوامر

يوفر هذا القسم معلومات حول كيفية التحكم في التطبيق في موجه الأوامر.

الاتصال بالدعم الفني

يوفر هذا القسم معلومات حول كيفية الاتصال بالدعم الفني في Kaspersky Lab.

المصطلحات

يحتوي هذا القسم على قائمة بالمصطلحات المذكورة في المستند وتعريفاتها.

Kaspersky Lab ZAO

يوفر هذا القسم معلومات حول Kaspersky Lab.

معلومات حول التعليمات البرمجية الخاصة بطرف ثالث

يوفر هذا القسم معلومات حول الرمز الخاص بالطرف الخارجي والمستخدم في التطبيق.

إشعارات العلامة التجارية

يسرد هذا القسم العلامات التجارية الخاصة بجهات التصنيع الخارجية والمستخدمة في المستند.

فهرس

يتيح لك هذا القسم العثور على المعلومات المطلوبة في المستند بسرعة.

اصطلاحات المستند

يتضمن نص المستند عناصر دلالية نوصيك بالانتباه لها على وجه الخصوص، وهي: التحذيرات، والتلميحات، والأمثلة.

يتم استخدام اصطلاحات الوثيقة لتمييز العناصر الدلالية. يوضح الجدول التالي اصطلاحات الوثيقة وأمثلة لاستخدامها.

Table 1. اصطلاحات المستند

نص عينة	وصف اصطلاح المستند
لاحظ...	يتم تمييز التحذيرات باللون الأحمر وتوضع في مربع. توفر التحذيرات معلومات حول الإجراءات المحتملة غير المرغوب فيها، والتي قد تؤدي إلى فقدان البيانات، أو تعطل تشغيل الأجهزة، أو مشكلات في نظام التشغيل.
نوصيك باستخدام...	يتم وضع الملاحظات في مربع. قد تحتوي الملاحظات على تلميحات مفيدة أو توصيات أو قيم معينة للإعدادات أو حالات خاصة مهمة في تشغيل التطبيق.
مثال: ...	تظهر الأمثلة فوق خلفية صفراء تحت العنوان "مثال".

نص عينة	وصف اصطلاح المستند
تحديث يعني... قواعد *البيانات قديمة* وقوع حدث.	يتم كتابة العناصر الدلالية التالية بالخط المائل في النص: • المصطلحات الجديدة • أسماء حالات وأحداث التطبيق
اضغط إدخال. اضغط على **ALT+F4**.	تظهر أسماء مفاتيح لوحة المفاتيح بخط عريض وبأحرف كبيرة. أسماء مفاتيح لوحة المفاتيح المتصلة بعلامة "+" (زائد) تشير إلى استخدام توليفة مفاتيح. يجب الضغط على هذه المفاتيح في آن واحد.
انقر فوق زر تمكين.	يتم تمييز أسماء عناصر واجهة التطبيق، مثل حقول الإدخال وعناصر القائمة والأزرار بالخط العريض.
لتكوين جدولة المهمة:	يتم كتابة العبارات الافتتاحية في التعليمات بحروف مائلة وتكون مصحوبة بعلامة سهم.
في سطر الأوامر، أدخل help. ستظهر بعد ذلك الرسالة التالية: حدد التاريخ بتنسيق يوم / شهر / سنة.	يتم تمييز الأنواع التالية من المحتوى النصي بكتابتها بخط خاص: • نص في سطر الأوامر • نص الرسائل الذي يعرضه التطبيق على الشاشة • البيانات التي يجب أن يدخلها المستخدم
<اسم المستخدم>	يتم وضع المتغيرات داخل أقواس زاوية. بدلاً من المتغير، أدخل القيمة المناسبة دون تضمين الأقواس السهمية.

مصادر المعلومات المتعلقة بالتطبيق

يصف هذا القسم مصادر المعلومات المتعلقة بالتطبيق ويسرد مواقع الويب التي يمكنك استخدامها لمناقشة استخدام التطبيق.

يمكنك تحديد أنسب مصدر معلومات، وفقًا لمستوى أهمية وضرورة المشكلة.

في هذا القسم

مصادر معلومات البحث المستقل

يمكنك الاتصال بالمصادر التالية للمعلومات للبحث بنفسك:

- صفحة التطبيق على موقع Kaspersky Lab
- صفحة التطبيق على موقع الدعم الفني (قاعدة المعارف)
- تعليمات عبر الإنترنت
- وثائق

إذا تعذر عليك العثور على حل لمشكلتك، فنوصيك بالاتصال بالدعم الفني في Kaspersky Lab (راجع القسم "الدعم الفني عبر الهاتف" على صفحة 97).

يلزم وجود اتصال بالإنترنت لاستخدام موارد المعلومات الموجودة على موقع Kaspersky Lab على الويب.

صفحة التطبيق على موقع Kaspersky Lab

يشتمل موقع Kaspersky Lab على صفحة واحدة لكل تطبيق على حدة.

في هذه الصفحة (http://www.kaspersky.com/total-security-multi-device) يمكنك عرض معلومات عامة حول التطبيق، ووظائفه، ومزاياه.

تحتوي الصفحة على رابط يؤدي إلى eStore. حيث يمكنك شراء التطبيق أو تجديده فيه.

صفحة التطبيق على موقع الدعم الفني (قاعدة المعارف)

قاعدة المعارف هي قسم في موقع الدعم الفني على الويب يوفر نصائح حول استخدام تطبيقات Kaspersky Lab. تتكون "قاعدة المعارف" من مقالات مرجعية يتم تجميعها حسب الموضوع.

في صفحة التطبيق في قاعدة المعارف (http://support.kaspersky.com/kts) يمكنك قراءة مقالات تقدم معلومات مفيدة، وتوصيات، وإجابات عن الأسئلة المتكررة حول كيفية شراء التطبيق، وتثبيته، واستخدامه.

قد توفر المقالات إجابات عن الأسئلة التي تتعلق بتطبيق Kaspersky Total Security وتطبيقات Kaspersky Lab الأخرى. وقد تحتوي أيضًا على أخبار من الدعم الفني.

تعليمات عبر الإنترنت

تحتوي التعليمات عبر الإنترنت الخاصة بالتطبيق على ملفات للمساعدة.

توفر التعليمات السياقية معلومات حول كل نافذة من نوافذ التطبيق، حيث إنها تقوم بإدراج الإعدادات الملائمة وقائمة المهام كما تقدم وصفًا لها.

توفر التعليمات الكاملة معلومات مفصلة حول إدارة حماية الكمبيوتر، وتكوين التطبيق، وحل مشكلات المهام النموذجية التي يقوم بها المستخدم.

وثائق

يوفر دليل مستخدم التطبيق معلومات حول كيفية تثبيت التطبيق، وتفعيله، وتكوينه، بالإضافة إلى معلومات حول استخدام التطبيق. يصف أيضًا هذا المستند واجهة التطبيق ويوفر طرقًا لحل مشكلات المهام النموذجية التي يقوم بها المستخدم أثناء استخدام التطبيق.

مناقشة تطبيقات Kaspersky Lab في المنتدى

إذا لم يكن سؤالك يتطلب توفير إجابة فورية، فيمكنك مناقشته مع خبراء Kaspersky Lab والمستخدمين الآخرين في المنتدى الخاص بنا (http://forum.kaspersky.com).

في هذا المنتدى، يمكنك عرض الموضوعات الموجودة، وترك تعليقاتك، وإنشاء موضوعات جديدة للمناقشة.

KASPERSKY TOTAL SECURITY

يصف هذا القسم مزايا التطبيق ويقدم معلومات موجزة حول وظائف التطبيق ومكوناته. ستتعرف على العناصر المضمنة في حزمة التوزيع والخدمات المتوفرة للمستخدمين المسجلين للتطبيق. يوفر هذا القسم معلومات حول متطلبات البرامج والأجهزة التي يجب أن يفي بها الكمبيوتر حتى يتمكن المستخدم من تثبيت التطبيق عليه.

في هذا القسم

ما الجديد

يوفر Kaspersky Total Security المزايا الجديدة التالية:

- تمت إضافة تحذيرات المستخدم عند الاتصال بشبكات Wi-Fi غير محمية.
- تمت إضافة وظائف حظر الوصول غير المصرح به إلى كاميرا الويب. يتم منع الوصول إلى تدفقات فيديو كاميرا الويب.
- تمت إضافة حماية البيانات في الحافظة من السرقة والاعتراض.
- تمت إضافة خيار للتبديل إلى Kaspersky Anti-Virus أو Kaspersky Internet Security.
- يمكنك الآن إدارة حماية الأجهزة عن بُعد عبر مدخل My Kaspersky.
- تم تحسين الحماية ضد لقطات الشاشة غير المصرح بها. يحميك Kaspersky Total Security الآن من لقطات الشاشة غير المصرح بها باستخدام DirectX® وOpenGL.
- تم تحسين وظائف مكون مراقب النظام: تم تنفيذ الحماية ضد أدوات التشفير. يقوم Kaspersky Total Security بإنشاء نسخ احتياطية للملفات قبل تشفيرها بواسطة أداة تشفير خبيثة. يتيح هذا استعادة هذه الملفات من نسخها الاحتياطية. يتم تخزين نسخ الملفات الاحتياطية في مجلد النظام للملفات المؤقتة. يتم تطبيق قيود معينة على هذه الوظيفة (راجع القسم "القيود والتحذيرات" على صفحة 104).
- تم تعزيز وظائف "الرقابة الأسرية": تمت توسعة قائمة مواقع الويب التي يغطيها البحث الآمن.
- تم تبسيط إعدادات تكوين الرقابة الأسرية والخدمات النقدية الآمنة ووضع التطبيقات الموثوق بها والنسخ الاحتياطي والاستعادة وتشفير البيانات.
- تم تحسين الحماية في وضع التطبيقات الموثوق بها: تمت الآن مراقبة التطبيقات في مرحلة مبكرة من بدء تشغيل نظام التشغيل كما تم تنفيذ حماية تطبيقات .NET.

- يتم الآن دعم أحدث الإصدارات من مستعرضات الويب الشائعة: تدعم مكونات الحماية (مثل مستشار Kaspersky لعناوين مواقع الويب والخدمات النقدية الآمنة) مستعرضات Mozilla™ و Firefox™ 29.x و x.30 و x.31 و Internet Explorer® 11 و Google Chrome™ 36.x.
- تم تحسين أداء التطبيق، كما تم تحسين استهلاك موارد الكمبيوتر.
- وقت أقل مطلوب لبدء التطبيق.
- تمت إضافة الدعم لتحديث Windows® 8.1.
- تم تحسين عملية ترقية المنتج.
- تم تقليل حجم حزمة توزيع التطبيق.

حزمة التوزيع

يمكنك شراء التطبيق بإحدى الطرق التالية:

- مغلف. موزع بواسطة المتاجر الخاصة بشركائنا.
- من متجر الإنترنت. يتم التوزيع في متاجر Kaspersky Lab عبر الإنترنت (مثل، http://www.kaspersky.com، في قسم متجر الإنترنت) أو عبر شركات الشركاء.

إذا قمت بشراء الإصدار المغلف من التطبيق، تحتوي حزمة التوزيع على العناصر التالية:

- ظرف محكم الإغلاق يحتوي على القرص المضغوط الخاص بالإعداد، والذي يحتوي على ملفات التطبيق وملفات الوثائق
- دليل مستخدم موجز مع رمز تفعيل
- اتفاقية الترخيص التي تنص على بنود استخدام التطبيق

قد يختلف محتوى حزمة التوزيع اعتمادًا على المنطقة التي يتم فيها توزيع التطبيق.

إذا قمت بشراء Kaspersky Total Security من متجر عبر الإنترنت، فإنك تقوم بنسخ التطبيق من موقع الويب الخاص بالمتجر. سيتم إرسال المعلومات المطلوبة لتفعيل التطبيق إليك، بما فيها رمز التفعيل، عن طريق البريد الإلكتروني بعد أن يتم استلام المبلغ الخاص بك.

لمزيد من التفاصيل حول طرق الشراء ومجموعة التوزيع، اتصل بإدارة المبيعات من خلال إرسال رسالة إلى sales@kaspersky.com.

ميزات التطبيقات الأساسية

يوفر Kaspersky Total Security حماية شاملة للكمبيوتر ضد التهديدات المعروفة والجديدة، وهجمات الشبكة والهجمات الاحتيالية، والبريد الإلكتروني غير المرغوب فيه. كما تتوفر وظائف ومكونات حماية مختلفة كجزء من Kaspersky Total Security من أجل تقديم الحماية الشاملة.

حماية جهاز الكمبيوتر

تم تصميم *مكونات الحماية* لحماية الكمبيوتر من التهديدات المعروفة والجديدة، وهجمات الشبكات والاحتيال، والبريد الإلكتروني غير المرغوب فيه. تتم معالجة كل نوع من التهديدات بواسطة مكون أمان فردي (انظر المزيد عن وصف المكونات في هذا القسم). ويمكن تمكين المكونات أو تعطيلها بصورة مستقلة عن بعضها بالإضافة إلى تكوين الإعدادات الخاصة بها.

بالإضافة إلى الحماية الفورية التي توفرها مكونات الأمان، نوصي بأن تقوم *بفحص* الكمبيوتر بانتظام بحثًا عن الفيروسات والبرامج الخبيثة الأخرى. وهذا أمر ضروري لتجنب أي احتمال لانتشار البرامج الضارة التي لم تكتشفها مكونات الحماية بسبب ضبط مستوى أمان منخفض أو لأسباب أخرى مثلاً.

للحفاظ على Kaspersky Total Security مُحدَّثًا، يجب عليك *تحديث* قواعد البيانات ووحدات التطبيق التي يستخدمها التطبيق.

ينبغي تنفيذ بعض المهام المعينة من وقتٍ لآخر (مثل إزالة تتبعات أنشطة المستخدم في نظام التشغيل) باستخدام *الأدوات والمعالجات المتقدمة*.

توفر مكونات الحماية التالية حراسة جهاز الكمبيوتر في الوقت الحقيقي:

فيما يلي وصف للمنطق الذي تتفاعل به مكونات الحماية عند ضبط Kaspersky Total Security على الوضع الموصى به من قِبل متخصصي Kaspersky Lab (أي مع إعدادات التطبيق الافتراضية).

مكافحة فيروسات الملفات

يقوم مكون مكافحة فيروسات الملفات بمنع إصابة نظام ملفات الكمبيوتر. يعمل المكون عند بدء نظام التشغيل، ويبقى بصورة مستمرة في ذاكرة الوصول العشوائي (RAM) الخاصة بالكمبيوتر، ويقوم بفحص كل الملفات التي يتم فتحها، أو حفظها، أو تشغيلها على الكمبيوتر فضلاً عن جميع محركات الأقراص المتصلة. يعترض برنامج Kaspersky Total Security جميع محاولات الوصول إلى أي ملف، كما أنه يفحص ذلك الملف بحثًا عن الفيروسات المعروفة والبرامج الخبيثة الأخرى. يتم السماح بالوصول اللاحق إلى الملف فقط إذا لم يكن هذا الملف مصابًا أو إذا تم تنظيفه بنجاح بواسطة التطبيق. إذا تعذر تنظيف ملف ما لأي سبب من الأسباب، فسيتم حذفه. ويتم نقل نسخة من الملف إلى "العزل" عند حدوث ذلك.

مكافحة فيروسات البريد

يقوم مكون مكافحة فيروسات البريد بفحص رسائل البريد الإلكتروني الواردة والصادرة على جهاز الكمبيوتر. يتم توفير رسالة البريد الإلكتروني للمستلم فقط إذا لم تتضمن أي كائنات خطرة.

مكافحة فيروسات الويب

يعترض مكون مكافحة فيروسات الويب استئناء البرامج النصية الموجودة في مواقع الويب ومنعها إذا ما شكلت تهديدًا. كما يراقب مكون مكافحة فيروسات الويب كل حركة مرور الويب ويمنع الوصول إلى مواقع الويب الخطيرة.

مكافحة فيروسات المراسلة الفورية

يضمن مكون مكافحة فيروسات المراسلة الفورية الاستخدام الآمن للمراسلة الفورية. ويعمل هذا المكون على حماية المعلومات الواردة إلى جهاز الكمبيوتر عن طريق بروتوكولات المراسلة الفورية. ويضمن مكون مكافحة فيروسات المراسلة الفورية التشغيل الآمن لمختلف تطبيقات المراسلة الفورية.

التحكم في التطبيق

يسجل المكون "التحكم في التطبيق" الإجراءات التي تنفذها التطبيقات في نظام التشغيل، ويدير أنشطة التطبيقات بناءً على المجموعة التي يخصصها المكون لها. ويتم تحديد مجموعة قواعد لكل مجموعة من التطبيقات. حيث يتم بواسطة هذه القواعد إدارة وصول التطبيقات إلى موارد نظام التشغيل المختلفة.

جدار الحماية

يضمن جدار الحماية أمانك عند استخدام الشبكات المحلية والإنترنت. يعمل المكون على تصفية جميع أنشطة شبكة الاتصال باستخدام نوعين من القواعد: *قواعد للتطبيقات* و*قواعد الحزمة*.

مراقبة شبكة الاتصال

مراقبة الشبكة هي أداة مصممة لمراقبة أنشطة الشبكة في الوقت الحقيقي.

مراقب النظام

يمكن استخدام مكون مراقب النظام للتراجع عن إجراءات البرامج الضارة في نظام التشغيل.

حاجب هجمات الشبكة

يتم تحميل حاجب هجمات شبكة الاتصال عند بدء نظام التشغيل، ويقوم بتتبع حركة شبكة الاتصال الواردة للأنشطة التي تعد مميزة وخاصة بهجمات شبكة الاتصال. عند اكتشاف محاولة هجوم على جهاز الكمبيوتر، يقوم برنامج Kaspersky Total Security بمنع جميع أنشطة الشبكة التي يقوم بها الكمبيوتر المهاجم ضد الكمبيوتر الخاص بك.

مكافحة البريد الإلكتروني غير المرغوب فيه

يندمج مكون مكافحة البريد الإلكتروني غير المرغوب فيه في عميل البريد المثبت على جهاز الكمبيوتر، ويفحص جميع رسائل البريد الإلكتروني الواردة بحثًا عن البريد الإلكتروني غير المرغوب فيه. ويتم تمييز جميع الرسائل المحتوية على بريد إلكتروني غير مرغوب فيه برأس خاصة. يمكنك تكوين مكون مكافحة البريد الإلكتروني غير المرغوب فيه بحيث يعالج رسائل البريد العشوائي بطريقة خاصة (فيقوم مثلا بحذفها تلقائيًا أو نقلها إلى مجلد خاص).

مكافحة الاحتيال

يتيح مكون "مكافحة الاحتيال" التحقق من عناوين مواقع الويب لمعرفة ما إذا كانت واردة ضمن قائمة عناوين مواقع الويب الاحتيالية. إن هذا المكون هو مكون مندمج مع مكون مكافحة فيروسات الويب، ومكون مكافحة البريد الإلكتروني غير المرغوب فيه، ومكون مكافحة فيروسات المراسلة الفورية.

مكافحة الشعارات

يقوم مكون مكافحة الشعارات بمنع الشعارات الإعلانية التي على مواقع الويب وفي واجهات التطبيق.

الخدمات النقدية الآمنة

توفر الخدمات النقدية الآمنة الحماية للبيانات السرية عند استخدام الخدمات البنكية وأنظمة الدفع على الإنترنت، كما أنها تحول دون سرقة الأصول عند إجراء عمليات الدفع على الإنترنت.

الإدخال الآمن للوحة المفاتيح

يوفر الإدخال الآمن للوحة المفاتيح الحماية من برامج رصد لوحة المفاتيح بالنسبة للبيانات الشخصية التي يتم إدخالها على مواقع الويب. تمنع لوحة المفاتيح الظاهرية حدوث أي تعرض للبيانات المدخلة على لوحة المفاتيح المادية وتحمي البيانات الشخصية من محاولات الاعتراض التي تستخدم لقطات الشاشة.

وضع التطبيقات الموثوقة

يحمي وضع التطبيقات الموثوقة أجهزة الكمبيوتر من التطبيقات التي قد تكون غير آمنة. عند تمكين وضع التطبيقات المثوقة، يسمح Kaspersky Total Security بتشغيل التطبيقات التي يتم تحديدها على أنها موثوقة فقط (على سبيل المثال، بالاستناد إلى معلومات عن التطبيق من شبكة أمان Kaspersky أو توقيع رقمي موثوق).

الرقابة الأسرية

تم تصميم مكون الرقابة الأسرية لحماية الأطفال والمراهقين من التهديدات المتعلقة باستخدام الكمبيوتر والإنترنت.

يتيح لك مكون الرقابة الأسرية وضع قيود مرنة على وصول مختلف المستخدمين إلى موارد وتطبيقات الإنترنت، كل حسب عمره. وعلاوة على ذلك، يسمح مكون الرقابة الأسرية بعرض التقارير الإحصائية المتعلقة بنشاطات المستخدمين الخاضعين للرقابة.

النسخ الاحتياطي والاستعادة

تم تصميم وظائف النسخ الاحتياطي واستعادة البيانات لحماية بياناتك من السرقة كنتيجة لإخفاقات الأجهزة. يمكن لـ Kaspersky Total Security إجراء نسخ احتياطية مجدولة للبيانات لمحركات الأقراص القابلة للإزالة ومخازن الشبكة وعبر الإنترنت. يمكنك نسخ الملفات حسب الفئة وتحديد عدد إصدارات نفس الملف للتخزين.

تشفير البيانات

تم تصميم تشفير البيانات لحماية البيانات السرية ضد الوصول غير المصرح به. يمكنك فتح مخزن بيانات وعرض محتوياته فقط بعد إدخال كلمة مرور.

إدارة حماية الكمبيوتر عن بُعد

إذا تم تثبيت Kaspersky Total Security على كمبيوتر ولديك حساب على مدخل My Kaspersky، فيمكنك إدارة حماية هذا الكمبيوتر عن بُعد.

خدمة المستخدمين

عن طريق الحصول على ترخيص للتطبيق، يمكنك الاستفادة من الخدمات التالية أثناء فترة صلاحية الترخيص:

- تحديثات قواعد البيانات والوصول إلى الإصدارات الجديدة من التطبيق
- الاستشارات عبر الهاتف وعبر البريد الإلكتروني حول المشكلات المتعلقة بتثبيت التطبيق، وتكوينه، واستخدامه
- إخطارات بطرح التطبيقات الجديدة من Kaspersky Lab، وكذلك إخطارات بالفيروسات الجديدة وانتشار الفيروسات. لاستخدام هذه الخدمة، اشترك في خدمة توصيل الأخبار من Kaspersky Lab على موقع الدعم الفني على الويب.

لا يتم تقديم استشارات حول المشكلات المتعلقة بأنظمة التشغيل أو بالبرامج والتقنيات التي تقدمها جهات خارجية.

متطلبات الأجهزة والبرامج

لضمان عمل Kaspersky Total Security، ينبغي أن يفي الكمبيوتر بالمتطلبات التالية:

متطلبات عامة:

- معالج Intel® Pentium® III بقدرة 1 جيجاهرتز 32 بت (x86) / 64 بت (x64) أو أحدث (أو معالج مكافئ متوافق).
- 480 ميجابايت مساحة فارغة على محرك القرص الثابت
- محرك أقراص CD-/DVD-ROM (للتثبيت من القرص المضغوط الخاص بالتثبيت)
- الوصول إلى الإنترنت (لتفعيل التطبيق ولتحديث قواعد البيانات والوحدات البرمجية)

- Internet Explorer 8.0 أو أحدث
- Microsoft® Windows Installer 3.0 أو أحدث
- Microsoft .NET Framework 4 أو أحدث
- يتم توفير حماية الوصول إلى كاميرا الويب فقط لطرز كاميرا الويب المتوافقة http://support.kaspersky.com/10978.

متطلبات Microsoft Windows XP Home Edition (Service Pack 3 أو أحدث)، و Microsoft Windows XP Professional (Service Pack 3 أو أحدث)، و Microsoft Windows XP Professional x64 Edition (Service Pack 2 أو أحدث):

- 512 ميجابايت كمساحة خالية بذاكرة الوصول العشوائي (RAM)

متطلبات أنظمة التشغيل Microsoft Windows Vista® Home Basic (Service Pack 1 أو أحدث) و Microsoft Windows Vista Home Premium (Service Pack 1 أو أحدث) و Microsoft Windows Vista Business (Service Pack 1 أو أحدث) و Microsoft Windows Vista Enterprise (Service Pack 1 أو أحدث) و Microsoft Windows Vista Ultimate (Service Pack 1 أو أحدث) و Microsoft Windows 7 Starter (Service Pack 1 أو أحدث) و Microsoft Windows 7 Home Basic (Service Pack 1 أو أحدث) و Microsoft Windows 7 Home Premium (Service Pack 1 أو أحدث) و Microsoft Windows 7 Professional (Service Pack 1 أو أحدث)، و Microsoft Windows 7 Ultimate (Service Pack 1 أو أحدث) و Microsoft Windows 8 و Microsoft Windows 8 Pro و Microsoft Windows 8 Enterprise و Microsoft Windows 8.1 (Windows 8.1 Update) و Windows 8.1 Pro (Windows 8.1 Update) و Windows 8.1 Enterprise (Windows 8.1 Update):

- 1 جيجابايت كمساحة خالية بذاكرة الوصول العشوائي (RAM) (لأنظمة التشغيل 32 بت)؛ 2 جيجابايت كمساحة خالية بذاكرة الوصول العشوائي (RAM) (لأنظمة التشغيل 64 بت)

متطلبات أجهزة الكمبيوتر اللوحية:

- الكمبيوتر اللوحي من Microsoft
- وحدة معالجة مركزية (CPU) Intel Celeron® بسرعة 1،66 جيجاهرتز أو أعلى
- 1000 ميجابايت كمساحة خالية بذاكرة الوصول العشوائي (RAM)

المتطلبات لأجهزة كمبيوتر الإنترنت:

- وحدة معالجة مركزية (CPU) Intel Atom™ بسرعة 1،60 جيجاهرتز أو أعلى
- 1024 ميجابايت كمساحة خالية بذاكرة الوصول العشوائي (RAM)
- شاشة 10.1 بوصات بدقة 1024 × 600
- وحدة رسومات Intel GMA 950

تثبيت التطبيق وإزالته

يحتوي هذا القسم على إرشادات خطوة بخطوة لتثبيت التطبيق وإزالته.

في هذا القسم

إجراء التثبيت القياسي

سيتم تثبيت برنامج Kaspersky Total Security على جهاز الكمبيوتر في وضع تفاعلي باستخدام معالج التثبيت.

يتكون "المعالج" من سلسلة من الصفحات (الخطوات) التي يمكنك التنقل بينها بالنقر فوق الزرين **رجوع** و**التالي**. لإغلاق "المعالج" بعد انتهائه، انقر فوق الزر **إنهاء**. لإيقاف نشاط "المعالج" عند أي خطوة من خطوات التثبيت، أغلق نافذة "المعالج".

إذا كان التطبيق سيتم استخدامه لحماية أكثر من كمبيوتر واحد (وفقًا للحد الأقصى لعدد أجهزة الكمبيوتر الذي تحدده بنود اتفاقية ترخيص المستخدم النهائي)، فيكون إجراء التثبيت متطابقًا على جميع أجهزة الكمبيوتر.

تثبيت Kaspersky Total Security على الكمبيوتر:

من القرص الصلب الخاص بالتثبيت، قم بتشغيل حزمة التثبيت (الملف بامتداد .exe).

لتثبيت Kaspersky Total Security، يمكنك أيضًا استخدام حزمة تثبيت تم تنزيلها من الإنترنت. في هذه الحالة، يعرض "معالج الإعداد" خطوات تثبيت إضافية لبعض لغات الترجمة.

وبجوار التطبيق، يتم تثبيت المكونات الإضافية الخاصة بالمستعرضات للتأكد من سلامة تصفح الإنترنت.

في هذا القسم

الخطوة 1. البحث عن إصدار أحدث من التطبيق

قبل الإعداد، يقوم معالج التثبيت بفحص خوادم التحديث من Kaspersky Lab بحثًا عن إصدار أحدث من برنامج Kaspersky Total Security.

في حالة عدم اكتشاف معالج الإعداد لأي إصدار جديد من التطبيق على خوادم تحديث Kaspersky Lab، يبدأ في تثبيت الإصدار الحالي.

في حالة اكتشاف معالج الإعداد لإصدار أحدث من Kaspersky Total Security على خوادم تحديث Kaspersky Lab، فإنه يطالبك بتنزيله وتثبيته على الكمبيوتر. يوصى بتثبيت الإصدار الحديث من التطبيق، لأن الإصدارات الأحدث تتضمن المزيد من التحسينات التي تسمح لك بضمان الحصول على حماية أفضل للكمبيوتر الخاص بك. في حالة رفضك لتثبيت الإصدار الجديد، يبدأ المعالج في تثبيت الإصدار الحالي من التطبيق. إذا وافقت على تثبيت الإصدار الجديد من التطبيق، فيقوم معالج الإعداد بنسخ الملفات من حزمة التثبيت إلى الكمبيوتر الخاص بك ويبدأ في تثبيت الإصدار الجديد. لمزيد من التفاصيل حول كيفية تثبيت الإصدار الجديد من التطبيق، ارجع إلى الوثائق ذات الصلة.

الخطوة 2. بدء تثبيت التطبيق

في هذه الخطوة، يعرض عليك "معالج الإعداد" تثبيت التطبيق.

لمتابعة التثبيت، انقر فوق الزر **تثبيت**.

حسب نوع التثبيت ولغة الترجمة، يعرض عليك "معالج الإعداد" في هذه الخطوة إمكانية عرض "اتفاقية الترخيص" المبرمة بينك وبين Kaspersky Lab، كما أنه يسألك عن رغبك فيما إذا كنت تريد المشاركة في "شبكة أمان Kaspersky" أم لا.

الخطوة 3. مراجعة اتفاقية الترخيص

يتم عرض هذه الخطوة من المعالج لبعض لغات الترجمة عند تثبيت Kaspersky Total Security من حزمة التثبيت التي تم تنزيلها من الإنترنت.

في هذه الخطوة، يطلب منك "معالج الإعداد" مراجعة "اتفاقية الترخيص" المبرمة بينك وبين Kaspersky Lab.

قم بقراءة اتفاقية الترخيص جيدًا، إذا كنت توافق على جميع الشروط الخاصة بها، انقر فوق الزر **قبول**. ثم تتم مواصلة عملية تثبيت التطبيق على الكمبيوتر.

في حالة عدم قبول بنود اتفاقية الترخيص لن يتم تثبيت التطبيق.

الخطوة 4. بيان شبكة أمان KASPERSKY

في هذه الخطوة، يدعوك "معالج الإعداد" إلى المشاركة في "شبكة أمان Kaspersky". تتضمن المشاركة في البرنامج إرسال معلومات حول التهديدات الجديدة المكتشفة على الكمبيوتر الخاص بك والتطبيقات الموجودة قيد التشغيل والتطبيقات الموقعة المنزلة، بالإضافة إلى معلومات حول نظام التشغيل إلى Kaspersky Lab. لا يتم تجميع أو معالجة أو تخزين أي بيانات خاصة مستلمة.

راجع "بيان شبكة أمان Kaspersky". إذا كنت تقبل جميع بنوده، فانقر فوق الزر **قبول** في نافذة "المعالج".

إذا كنت لا تريد المشاركة في شبكة أمان Kaspersky، فانقر فوق الزر **رفض** .

بعد قبولك المشاركة في "شبكة أمان Kaspersky" أو رفضها، تتم مواصلة عملية تثبيت التطبيق.

الخطوة 5. التثبيت:

يتم توزيع بعض الإصدارات من Kaspersky Total Security باشتراكات، ويجب إدخال كلمة المرور التي استلمتها من موفر الخدمة قبل تثبيت هذه الإصدارات.

بعد إدخالك كلمة المرور، يبدأ تثبيت التطبيق.

قد يستغرق تثبيت التطبيق بعض الوقت. الرجاء الانتظار حتى يكتمل.

عند اكتمال التثبيت، يتابع "معالج الإعداد" تلقائيًا إلى الخطوة التالية.

يقوم Kaspersky Total Security بتنفيذ عمليات فحص متعددة أثناء التثبيت. قد تكتشف هذه الفحوصات المشكلات التالية:

- عدم *توافق نظام التشغيل مع متطلبات البرامج*. أثناء التثبيت، يقوم المعالج بفحص الحالات التالية:
  - إيفاء نظام التشغيل وحزمة الخدمة بمتطلبات البرامج
  - توفر جميع التطبيقات المطلوبة
  - ما إذا كانت المساحة الحرة المتوفرة على القرص كافية للتثبيت.

  إذا لم يتم الإيفاء بأي من المتطلبات المدرجة أعلاه، فسيتم عرض الإخطار المناسب.
- توجد *تطبيقات غير متوافقة على الكمبيوتر*. إذا تم اكتشاف أي تطبيقات غير متوافقة فسيتم عرضها في قائمة معروضة على الشاشة، وسيطلب منك إزالتها. ننصحك بالإزالة اليدوية لأي تطبيقات يتعذر على Kaspersky Total Security إزالتها بشكل تلقائي. أثناء إزالة التطبيقات غير المتوافقة، سيتوجب عليك إعادة تمهيد نظام التشغيل، وبعد ذلك ستستمر عملية تثبيت برنامج Kaspersky Total Security تلقائيًا.
- *وجود برامج ضارة على الكمبيوتر*. إذا تم اكتشاف أي برامج ضارة - تتداخل مع تثبيت برنامج مكافحة الفيروسات - على الكمبيوتر، فسيطلب منك "معالج الإعداد" تنزيل *أداة إزالة الفيروسات من Kaspersky*، وهي عبارة عن أداة خاصة مصممة لإبطال الإصابات.

  إذا وافقت على تثبيت الأداة المساعدة، فإن معالج التثبيت سيقوم بتحميلها من خوادم Kaspersky Lab وبعد ذلك يبدأ في تثبيت الأداة تلقائيًا. إذا تعذر على "المعالج" تنزيل الأداة، فسيُطلب منك تنزيلها بنفسك عن طريق النقر فوق الرابط الذي تم توفيره إليك.

الخطوة 6. إكمال التثبيت

في هذه الخطوة، يخبرك "المعالج" باكتمال تثبيت التطبيق. لبدء استخدام Kaspersky Total Security على الفور، تأكد من تحديد خانة الاختيار **تشغيل Kaspersky Total Security**، وانقر فوق الزر **إنهاء**.

في حالة عدم تحديد خانة الاختيار **تشغيل Kaspersky Total Security** قبل إغلاق "المعالج"، ستحتاج إلى تشغيل التطبيق يدويًا.

في بعض الحالات، قد تحتاج إلى إعادة تشغيل نظام التشغيل لإكمال التثبيت.

الخطوة 7. تفعيل التطبيق

في هذه الخطوة، يطلب منك "معالج الإعداد" تفعيل التطبيق.

التفعيل هو عملية تشغيل إصدار كامل الوظائف من التطبيق لفترة زمنية معينة.

إذا قمت بشراء ترخيص لـ Kaspersky Total Security وقمت بتنزيل التطبيق من متجر عبر الإنترنت، فيمكن تفعيل التطبيق تلقائيًا أثناء عملية التثبيت.

تُعرض عليك الخيارات التالية لتفعيل Kaspersky Total Security:

- **تفعيل التطبيق**. حدد هذا الخيار، وأدخل رمز التفعيل إذا اشتريت ترخيصًا للتطبيق.

  إذا حددت رمز تفعيل لـ Kaspersky Internet Security أو Kaspersky Anti-Virus في حقل الإدخال، فسيبدأ إجراء التبديل إلى Kaspersky Internet Security أو Kaspersky Anti-Virus بعد اكتمال عملية التفعيل.

- **تفعيل الإصدار التجريبي من التطبيق**. حدد خيار التفعيل هذا إذا أردت تثبيت الإصدار التجريبي من التطبيق قبل اتخاذ قرار بشأن شراء ترخيص. سوف تكون قادرًا على استخدام التطبيق، وجميع ميزاته أثناء فترة تقييم قصيرة. عند انتهاء صلاحية الترخيص التجريبي، لا يمكن تفعيل الإصدار التجريبي من التطبيق مرة ثانية.

يلزم الاتصال بالإنترنت لتفعيل التطبيق.

أثناء تفعيل التطبيق، قد يتعين عليك التسجيل على مدخل My Kaspersky.

الخطوة 8. تسجيل المستخدم

هذه الخطوة متاحة في بعض إصدارات Kaspersky Total Security.

يستطيع المستخدمون المسجلون إرسال طلبات إلى الدعم الفني ومعمل مكافحة الفيروسات من خلال مدخل My Kaspersky وإدارة رموز التفعيل بسهولة واستلام أحدث المعلومات الخاصة بالتطبيقات الجديدة والعروض الخاصة من Kaspersky Lab.

إذا وافقت على التسجيل، قم بتحديد بيانات التسجيل في الحقول المقابلة ثم النقر فوق الزر **التالي** لإرسال البيانات إلى Kaspersky Lab.

في بعض الحالات يلزم تسجيل المستخدم لبدء استخدام التطبيق.

الخطوة 9. إكمال التفعيل

يقوم المعالج بإخطارك بنجاح تنشيط Kaspersky Total Security. يتم أيضًا توفير معلومات حول الترخيص الحالي في هذه النافذة: تاريخ انتهاء صلاحية الترخيص وعدد أجهزة المضيفة التي يغطيها الترخيص.

إذا كنت قد قمت بطلب الاشتراك، فسيتم عرض المعلومات عن حالة الاشتراك بدلاً من تاريخ انتهاء الترخيص.

انقر الزر **إنهاء** لإغلاق المعالج.

ترقية إصدار سابق من التطبيق

تثبيت Kaspersky Total Security فوق Kaspersky PURE

إذا تم تثبيت Kaspersky PURE على الكمبيوتر بالفعل، فيمكنك ترقيته إلى Kaspersky Total Security. إذا كان لديك ترخيص حالي لبرنامج Kaspersky PURE، فلن تضطر إلى تفعيل التطبيق: سيقوم معالج الإعداد تلقائيًا باسترداد المعلومات الخاصة بترخيص Kaspersky PURE وتطبيقها خلال عملية تثبيت Kaspersky Total Security.

تثبيت Kaspersky Total Security فوق Kaspersky Internet Security

إذا قمت بتثبيت Kaspersky Total Security على كمبيوتر مثبت عليه بالفعل Kaspersky Internet Security مع وجود ترخيص صالح، فيطالبك معالج التفعيل بتحديد أحد الخيارات التالية:

- استمر في استخدام Kaspersky Internet Security بموجب الترخيص الحالي. وفي هذه الحالة، سيتم بدء معالج الترحيل. عند انتهاء "معالج الترحيل"، سيتم تثبيت Kaspersky Internet Security على الكمبيوتر. يمكنك استخدام Kaspersky Internet Security حتى تنتهي صلاحية الترخيص الخاص به.
- تابع مع عملية تثبيت الإصدار الجديد من Kaspersky Total Security. في هذه الحالة، سيتم تثبيت التطبيق وتفعيله بناءً على السيناريو القياسي.

سيتم تثبيت برنامج Kaspersky Total Security على جهاز الكمبيوتر في وضع تفاعلي باستخدام معالج التثبيت.

يتكون "المعالج" من سلسلة من الصفحات (الخطوات) التي يمكنك التنقل بينها بالنقر فوق الزرين **رجوع** و**التالي**. لإغلاق "المعالج" بعد انتهائه، انقر فوق الزر **إنهاء**. لإيقاف نشاط "المعالج" عند أي خطوة من خطوات التثبيت، أغلق نافذة "المعالج".

إذا كان التطبيق سيتم استخدامه لحماية أكثر من كمبيوتر واحد (وفقًا للحد الأقصى لعدد أجهزة الكمبيوتر الذي تحدده بنود اتفاقية ترخيص المستخدم النهائي)، فيكون إجراء التثبيت متطابقًا على جميع أجهزة الكمبيوتر.

لتثبيت Kaspersky Total Security على الكمبيوتر:

من القرص الصلب الخاص بالتثبيت، قم بتشغيل حزمة التثبيت (الملف بامتداد .exe).

لتثبيت Kaspersky Total Security، يمكنك أيضًا استخدام حزمة تثبيت تم تنزيلها من الإنترنت. في هذه الحالة، يعرض "معالج الإعداد" خطوات تثبيت إضافية لبعض لغات الترجمة.

وبجوار التطبيق، يتم تثبيت المكونات الإضافية الخاصة بالمستعرضات للتأكد من سلامة تصفح الإنترنت.

يتم تطبيق قيود معينة على الترقية من الإصدار السابق (انظر القسم "القيود والتحذيرات" على صفحة 104).

في هذا القسم

الخطوة 1. البحث عن إصدار أحدث من التطبيق

قبل الإعداد، يقوم معالج التثبيت بفحص خوادم التحديث من Kaspersky Lab بحثًا عن إصدار أحدث من برنامج Kaspersky Total Security.

في حالة عدم اكتشاف معالج الإعداد لأي إصدار جديد من التطبيق على خوادم تحديث Kaspersky Lab، يبدأ في تثبيت الإصدار الحالي.

في حالة اكتشاف معالج الإعداد لإصدار أحدث من Kaspersky Total Security على خوادم تحديث Kaspersky Lab، فإنه يطالبك بتنزيله وتثبيته على الكمبيوتر. يوصى بتثبيت الإصدار الحديث من التطبيق، لأن الإصدارات الأحدث تتضمن المزيد من التحسينات التي تسمح لك بضمان الحصول على حماية أفضل للكمبيوتر الخاص بك. في حالة رفضك لتثبيت الإصدار الجديد، يبدأ المعالج في تثبيت الإصدار الحالي من التطبيق. إذا وافقت على تثبيت الإصدار الجديد من التطبيق، فيقوم معالج الإعداد بنسخ الملفات من حزمة التثبيت إلى الكمبيوتر الخاص بك ويبدأ في تثبيت الإصدار الجديد. لمزيد من التفاصيل حول كيفية تثبيت الإصدار الجديد من التطبيق، ارجع إلى الوثائق ذات الصلة.

الخطوة 2. بدء تثبيت التطبيق

في هذه الخطوة، يعرض عليك "معالج الإعداد" تثبيت التطبيق.

لمتابعة التثبيت، انقر فوق الزر **تثبيت**.

حسب نوع التثبيت ولغة الترجمة، يعرض عليك "معالج الإعداد" في هذه الخطوة إمكانية عرض "اتفاقية الترخيص" المبرمة بينك وبين Kaspersky Lab، كما أنه يسألك عن رغبك فيما إذا كنت تريد المشاركة في "شبكة أمان Kaspersky" أم لا.

الخطوة 3. مراجعة اتفاقية الترخيص

يتم عرض هذه الخطوة من المعالج لبعض لغات الترجمة عند تثبيت Kaspersky Total Security من حزمة التثبيت التي تم تنزيلها من الإنترنت.

في هذه الخطوة، يطلب منك "معالج الإعداد" مراجعة "اتفاقية الترخيص" المبرمة بينك وبين Kaspersky Lab.

قم بقراءة اتفاقية الترخيص جيدًا، إذا كنت توافق على جميع الشروط الخاصة بها، انقر فوق الزر **قبول**. ثم تتم مواصلة عملية تثبيت التطبيق على الكمبيوتر.

في حالة عدم قبول بنود اتفاقية الترخيص لن يتم تثبيت التطبيق.

الخطوة 4. بيان شبكة أمان KASPERSKY

في هذه الخطوة، يدعوك "معالج الإعداد" إلى المشاركة في "شبكة أمان Kaspersky". تتضمن المشاركة في البرنامج إرسال معلومات حول التهديدات الجديدة المكتشفة على الكمبيوتر الخاص بك والتطبيقات الموجودة قيد التشغيل والتطبيقات الموقعة المنزلة، بالإضافة إلى معلومات حول نظام التشغيل إلى Kaspersky Lab. لا يتم تجميع أو معالجة أو تخزين أي بيانات خاصة مستلمة.

راجع "بيان شبكة أمان Kaspersky". إذا كنت تقبل جميع بنوده، فانقر فوق الزر **قبول** في نافذة "المعالج".

إذا كنت لا تريد المشاركة في شبكة أمان Kaspersky، فانقر فوق الزر **رفض** .

بعد قبولك المشاركة في "شبكة أمان Kaspersky" أو رفضها، تتم مواصلة عملية تثبيت التطبيق.

الخطوة 5. التثبيت:

يتم توزيع بعض الإصدارات من Kaspersky Total Security باشتراكات، ويجب إدخال كلمة المرور التي استلمتها من موفر الخدمة قبل تثبيت هذه الإصدارات.

بعد إدخالك كلمة المرور، يبدأ تثبيت التطبيق.

قد يستغرق تثبيت التطبيق بعض الوقت. الرجاء الانتظار حتى يكتمل.

عند اكتمال التثبيت، يتابع "معالج الإعداد" تلقائيًا إلى الخطوة التالية.

يقوم Kaspersky Total Security بتنفيذ عمليات فحص متعددة أثناء التثبيت. قد تكتشف هذه الفحوصات المشكلات التالية:

- عدم *توافق نظام التشغيل مع متطلبات البرامج*. أثناء التثبيت، يقوم المعالج بفحص الحالات التالية:
  - إيفاء نظام التشغيل وحزمة الخدمة بمتطلبات البرامج
  - توفر جميع التطبيقات المطلوبة
  - ما إذا كانت المساحة الحرة المتوفرة على القرص كافية للتثبيت.

  إذا لم يتم الإيفاء بأي من المتطلبات المدرجة أعلاه، فسيتم عرض الإخطار المناسب.
- *توجد تطبيقات غير متوافقة على الكمبيوتر*. إذا تم اكتشاف أي تطبيقات غير متوافقة فسيتم عرضها في قائمة معروضة على الشاشة، وسيطلب منك إزالتها. ننصحك بالإزالة اليدوية لأي تطبيقات يتعذر على Kaspersky Total Security إزالتها بشكل تلقائي. أثناء إزالة التطبيقات غير المتوافقة، سيتوجب عليك إعادة تمهيد نظام التشغيل، وبعد ذلك ستستمر عملية تثبيت برنامج Kaspersky Total Security تلقائيًا.
- *وجود برامج ضارة على الكمبيوتر*. إذا تم اكتشاف أي برامج ضارة - تتداخل مع تثبيت برنامج مكافحة الفيروسات - على الكمبيوتر، فسيطلب منك "معالج الإعداد" تنزيل *أداة إزالة الفيروسات من Kaspersky*، وهي عبارة عن أداة خاصة مصممة لإبطال الإصابات.

  إذا وافقت على تثبيت الأداة المساعدة، فإن معالج التثبيت سيقوم بتحميلها من خوادم Kaspersky Lab وبعد ذلك يبدأ في تثبيت الأداة تلقائيًا. إذا تعذر على "المعالج" تنزيل الأداة، فسيُطلب منك تنزيلها بنفسك عن طريق النقر فوق الرابط الذي تم توفيره إليك.

الخطوة 6. إكمال التثبيت

تخبرك هذه الصفحة من "معالج الإعداد" باكتمال تثبيت التطبيق بنجاح.

أعد تشغيل نظام التشغيل بعد أن يتم تثبيت التطبيق.

في حالة تحديد خانة الاختيار **تشغيل Kaspersky Total Security**، سيتم بدء التطبيق تلقائيًا بعد إعادة تشغيل الكمبيوتر.

في حالة عدم تحديد خانة الاختيار **تشغيل Kaspersky Total Security** قبل إغلاق "المعالج"، ستحتاج إلى تشغيل التطبيق يدويًا.

إزالة التطبيق

بعد إزالة Kaspersky Total Security، سيصبح الكمبيوتر والبيانات الخاصة غير محمية.

يتم إلغاء تثبيت برنامج Kaspersky Total Security بمساعدة معالج الإعداد.

➡ *لبدء "المعالج":*

في القائمة **ابدأ**، حدد **كافة البرامج** ◻ **Kaspersky Total Security** ◻ **إزالة Kaspersky Total Security**.

في هذا القسم

الخطوة 1. إدخال كلمة المرور لإزالة التطبيق

لإزالة Kaspersky Total Security، يجب إدخال كلمة المرور للوصول إلى إعدادات التطبيق. إذا تعذر عليك تحديد كلمة المرور لأي سبب كان، فسيتم منع إزالة التطبيق.

يتم عرض هذه الخطوة فقط إذا تم ضبط كلمة مرور لإزالة التطبيق.

الخطوة 2. حفظ البيانات للاستخدام في المستقبل

في هذه الخطوة، يمكنك تحديد أي من البيانات التي يستخدمها التطبيق تريد أن تحتفظ بها لاستخدامها لاحقًا أثناء التثبيت التالي للتطبيق (عند تثبيت إصدار أحدث من التطبيق مثلاً).

بشكل افتراضي، يعرض عليك التطبيق حفظ المعلومات حول الترخيص.

لحفظ البيانات لاستخدامها لاحقًا، حدد خانات الاختيار المجاورة لأنواع البيانات التي تريد حفظها:

- **معلومات الترخيص** هي عبارة عن مجموعة من البيانات التي تحدد قواعد الحاجة إلى تفعيل التطبيق أثناء التثبيت مستقبلاً عن طريق السماح لك باستخدام الترخيص الحالي ما لم تنته صلاحية الترخيص قبل بدء التثبيت.
- **ملفات العزل** هي الملفات التي يتم فحصها بواسطة التطبيق ونقلها إلى "العزل".

بعد أن تتم إزالة Kaspersky Total Security من الكمبيوتر، تصبح الملفات المعزولة غير متوفرة. لإجراء عمليات مع هذه الملفات، يجب تثبيت Kaspersky Total Security.

- **الإعدادات التشغيلية للتطبيق** هي قيم إعدادات التطبيق المحددة أثناء التكوين.

لا تضمن Kaspersky Lab دعم إعدادات الإصدارات السابقة من التطبيق. بعد تثبيت الإصدار الجديد، نوصي بالتحقق من صحة إعداداته.

كما يمكنك تصدير إعدادات الحماية في موجه الأوامر باستخدام الأمر التالي:

avp.com EXPORT <file_name>

- تتكون **بيانات iChecker** من ملفات تصف الكائنات التي تم فحصها بالفعل باستخدام تقنية iChecker.
- **قواعد بيانات مكافحة البريد الإلكتروني غير المرغوب فيه** هي قواعد بيانات تحتوي على أمثلة لرسائل البريد الإلكتروني غير المرغوب فيها المستلمة والمحفوظة بواسطة التطبيق.

الخطوة 3. تأكيد إزالة التطبيق

نظرًا لأن إزالة التطبيق تهدد أمان الكمبيوتر وبياناتك الخاصة، سيُطلب منك تأكيد رغبتك في إزالة التطبيق. للقيام بذلك، انقر الزر **إزالة**.

الخطوة 4. إزالة التطبيق. استكمال الإزالة

في هذه الخطوة، يقوم "المعالج" بإزالة التطبيق من الكمبيوتر. الرجاء الانتظار حتى اكتمال عملية الإزالة.

بعد إزالة Kaspersky Total Security، يمكنك تحديد السبب وراء قرارك بإزالة التطبيق، وذلك من خلال ترك تعليق على موقع Kaspersky Lab على الويب. للقيام بهذا، تفضل بزيارة موقع Kaspersky Lab على الويب بالنقر فوق الزر **أكمل النموذج**.

أثناء إزالة التطبيق، يجب إعادة تشغيل نظام التشغيل. إذا قمت بإلغاء إعادة التشغيل الفورية، فسيتم تأجيل إكمال إجراء الإزالة حتى تتم إعادة تشغيل نظام التشغيل أو يتم إيقاف تشغيل الكمبيوتر ثم يعاد تشغيله.

ترخيص التطبيق

يوفر هذا القسم معلومات حول البنود الأساسية المتعلقة بتفعيل التطبيق. اقرأ هذا القسم لتتعرف على المزيد حول الهدف من "اتفاقية ترخيص المستخدم النهائي"، وطرق تفعيل التطبيق، وتجديد الترخيص.

في هذا القسم

حول اتفاقية ترخيص المستخدم النهائي

اتفاقية ترخيص المستخدم النهائي هي اتفاقية إلزامية بينك وبين Kaspersky Lab ZAO تحدد البنود التي يمكنك بموجبها استخدام التطبيق.

قم بقراءة البنود والشروط الخاصة باتفاقية الترخيص بعناية قبل أن تقوم ببدء استخدام التطبيق.

تُعتبر موافقًا على بنود اتفاقية الترخيص بعد تأكيد موافقتك على اتفاقية الترخيص عند تثبيت التطبيق. إذا كنت لا تقبل بنود "اتفاقية الترخيص"، فيجب أن تقوم بإنهاء عملية تثبيت التطبيق ولا تستخدم التطبيق.

حول الترخيص

الترخيص هو حق استخدام التطبيق لفترة زمنية محدودة، والذي يتم منحه بموجب اتفاقية ترخيص المستخدم النهائي. يتعلق الترخيص بالرمز الفريد الخاص بتفعيل نسخة Kaspersky Total Security.

يمنحك الترخيص الحق في التمتع بأنواع الخدمات التالية:

- الحق في استخدام التطبيق على جهاز واحد أو عدة أجهزة

  يتم تحديد عدد الأجهزة التي قد تستخدم التطبيق عليها في اتفاقية ترخيص المستخدم النهائي.

- الحصول على المساعدة من "دعم Kaspersky Lab الفني"
- تتوفر خدمات أخرى من Kaspersky Lab أو شركائها أثناء فترة الترخيص (راجع قسم "خدمة المستخدمين" في صفحة 18).

لتشغيل التطبيق، يجب شراء ترخيص لاستخدام التطبيق.

للترخيص له مدة محددة. عند انتهاء صلاحية الترخيص، يواصل التطبيق العمل، ولكن بوظائف محددة (فلا يمكنك تحديث التطبيق أو استخدام "شبكة اتصال أمان Kaspersky" على سبيل المثال). ولا يزال بإمكانك الاستفادة من جميع مكونات التطبيق وتنفيذ عمليات الفحص بحثًا عن الفيروسات والبرمجيات الضارة الأخرى، ولكن يتم ذلك فقط باستخدام قواعد بيانات التي تم تثبيتها قبل انتهاء صلاحية الترخيص. لمتابعة استخدام Kaspersky Total Security في وضع الوظائف الكاملة، ينبغي تجديد ترخيصك.

نوصيك بتجديد الترخيص قبل انتهاء صلاحيته لضمان أقصى حماية للكمبيوتر من جميع التهديدات الأمنية.

قبل شراء ترخيص، يمكنك الحصول على إصدار تجريبي مجاني من Kaspersky Total Security. يعمل الإصدار التجريبي من Kaspersky Total Security خلال فترة تقييم قصيرة. بعد انتهاء فترة التقييم، يتم تعطيل جميع مزايا Kaspersky Total Security. لمتابعة استخدام التطبيق، يجب شراء ترخيص.

حول رمز التفعيل

رمز التفعيل هو رمز تستلمه عند شراء ترخيص لتطبيق Kaspersky Total Security. وهو مطلوب لتنشيط التطبيق.

يعتبر رمز التنشيط عبارة عن سلسلة فريدة مكونة من عشرين رقم وأحرف لاتينية في تنسيق xxxxx-xxxxx-xxxxx-xxxxx.

واعتمادًا على طريقة شراء التطبيق، يمكنك الحصول على رمز التنشيط بأي من الطرق التالية:

- عند شراء إصدار معلب من Kaspersky Total Security، يتم توفير رمز تفعيل في الدليل أو على علبة البيع بالتجزئة التي تتضمن القرص المضغوط الخاص بالتثبيت.
- عند شراء Kaspersky Total Security من متجر عبر الإنترنت، يتم إرسال رمز تفعيل عبر البريد الإلكتروني إلى العنوان الذي حددته عند طلب الشراء.

يبدأ العد التنازلي لفترة الترخيص من تاريخ تفعيل التطبيق. إذا اشتريت ترخيصًا لاستخدام Kaspersky Total Security على عدة أجهزة، فسيبدأ العد التنازلي لفترة الترخيص من لحظة قيامك بتطبيق رمز التفعيل لأول مرة.

في حالة فقدان رمز التفعيل أو حذفه دون قصد بعد تفعيل التطبيق، اتصل بدعم Kaspersky Lab الفني لاستعادة رمز التفعيل (http://support.kaspersky.com).

حول الاشتراك

يثبت *الاشتراك في Kaspersky Total Security* استخدام التطبيق ضمن المعلمات المحددة (تاريخ الانتهاء ورقم الأجهزة المحمية). يمكنك الحصول على اشتراك لبرنامج Kaspersky Total Security من أحد موفري الخدمة (من موفر خدمة الإنترنت لديك على سبيل المثال). يمكنك إيقاف اشتراكك مؤقتًا أو استئنافه، كما يمكنك تجديده تلقائيًا، أو إلغاؤه. يمكنك إدارة اشتراكك عبر صفحة حسابك الشخصي على موقع الويب الخاص بموفر الخدمة.

يستطيع موفرو الخدمة تقديم نوعين من اشتراكات Kaspersky Total Security: اشتراكات التحديث، واشتراكات التحديث والحماية.

يمكن أن يكون الاشتراك محدودًا (لمدة عام واحد مثلاً) أو غير محدود (بدون تاريخ لانتهاء الصلاحية). لمتابعة استخدام Kaspersky Total Security بعد انتهاء صلاحية الاشتراك المحدود، ينبغي تجديده. يتم تجديد الاشتراكات غير المحدودة تلقائيًا طالما يتم الدفع بشكل مسبق وفي الوقت المناسب إلى موفر الخدمة.

عند انتهاء صلاحية الاشتراك المحدود، يتم منحك فترة سماح لتجديد اشتراكك. وتبقى وظائف التطبيق دون تغيير خلال هذه الفترة.

إذا لم يتم تجديد الاشتراك قبل انتهاء فترة السماح، فسيقوم Kaspersky Total Security بإيقاف قواعد بيانات التطبيق (في حالة اشتراكات التحديث) أو إيقاف التفاعل مع Kaspersky Security Network، وأيضًا إيقاف حماية الكمبيوتر وتشغيل مهام الفحص (في حالة اشتراكات التحديث والحماية).

لاستخدام Kaspersky Total Security باشتراك، قم بتطبيق رمز التفعيل المستلم من موفر الخدمة. في بعض الحالات، سيتم تنزيل رمز التفعيل وتطبيقه تلقائيًا. عند استخدام التطبيق بموجب اشتراك، لا يمكنك تطبيق رمز تفعيل آخر لتجديد ترخيصك. يمكنك تطبيق رمز تفعيل آخر فقط عند انتهاء مدة الاشتراك.

إذا كان Kaspersky Total Security مستخدمًا بالفعل بموجب الترخيص الحالي عند قيامك بتسجيل اشتراكك، فسيتم استخدام Kaspersky Total Security بموجب الاشتراك بعد التسجيل. ويمكنك تطبيق رمز التفعيل - الذي استخدمته لتفعيل التطبيق - على كمبيوتر آخر.

لإلغاء اشتراكك، اتصل بموفر الخدمة الذي اشتريت منه Kaspersky Total Security.

وفقًا لموفر الاشتراك، قد تختلف مجموعة خيارات إدارة الاشتراك. علاوةً على ذلك، قد لا يتم منحك فترة سماح التي يمكنك خلالها تجديد اشتراكك.

حول توفير البيانات

لزيادة مستوى الحماية، أنت توافق على توفير المعلومات التالية تلقائيًا إلى Kaspersky Lab عند الموافقة على شروط اتفاقية الترخيص:

- معلومات حول المجاميع الاختبارية للملفات التي تتم معالجتها (MD5)
- المعلومات اللازمة لتقييم سمعة عناوين مواقع الويب
- إحصائيات حول استخدام إخطارات التطبيق
- بيانات إحصائية للحماية من البريد الإلكتروني غير المرغوب فيه
- بيانات التفعيل وإصدار Kaspersky Total Security المستخدم
- معلومات حول ترخيص الإصدار المُثبَّت من Kaspersky Total Security
- معلومات حول أنواع التهديدات المكتشفة
- معلومات حول الشهادات الرقمية المستخدمة حاليًا والمعلومات اللازمة للتحقق من صحتها
- تفاصيل تشغيل التطبيق والتراخيص المطلوبة لتكوين عرض محتوى مواقع الويب الموثوق بها

إذا كان الكمبيوتر مزوَّدًا بالوحدة النمطية للنظام الأساسي الموثوق به (TPM)، فإنك توافق أيضًا على تزويد Kaspersky Lab بتقرير TPM حول عملية بدء تشغيل نظام التشغيل والمعلومات اللازمة للتحقق من صحة التقرير. إذا حدث خطأ أثناء تثبيت Kaspersky Total Security، فإنك توافق على تزويد Kaspersky Lab تلقائيًا بمعلومات حول رمز الخطأ، وحزمة التثبيت المستخدمة حاليًا، والكمبيوتر لديك.

إذا كنت تشارك في شبكة اتصال أمان Kaspersky (انظر القسم "المشاركة في شبكة اتصال أمان Kaspersky (KSN)" على صفحة 94)، فأنت توافق على إرسال المعلومات التالية المتعلقة باستخدام Kaspersky Total Security من الكمبيوتر إلى Kaspersky Lab:

- معلومات حول المكونات المادية للكمبيوتر والبرامج المُثبَّتة عليه
- معلومات حول حالة حماية الكمبيوتر من الفيروسات، إلى جانب معلومات حول كل الكائنات محتملة الإصابة، والقرارات المتخذة بخصوص هذه الكائنات
- معلومات حول التطبيقات التي يتم تنزيلها وتشغيلها
- معلومات حول أخطاء واستخدام واجهة Kaspersky Total Security

- تفاصيل التطبيق، بما في ذلك إصدار التطبيق، والمعلومات حول ملفات الوحدات البرمجية التي يتم تنزيلها، وإصدارات قواعد بيانات التطبيق الحالية
- إحصائيات التحديثات والاتصالات بخوادم Kaspersky Lab
- معلومات حول الاتصال اللاسلكي المستخدم حاليًا
- إحصائيات حول الوقت الفعلي الذي تستغرقه مكونات التطبيق في فحص الكائنات
- إحصائيات حول التأخيرات المتعلقة بتطبيق Kaspersky Total Security عند بدء تشغيل التطبيقات
- الملفات التي قد يستخدمها المجرمون لإتلاف الكمبيوتر أو أجزاء من هذه الملفات، بما في ذلك الملفات التي يتم الرجوع إليها بواسطة الروابط الضارة

يمكن تخزين المعلومات المرسلة إلى Kaspersky Lab على الكمبيوتر حتى 30 يومًا بعد إنشائها. يتم الاحتفاظ بعناصر البيانات في مخزن داخلي محمي. الحد الأقصى لحجم البيانات التي يمكن تخزينها هو 30 ميجابايت.

علاوةً على ذلك، توافق على إرسال الملفات تلقائيًا (أو أجزاء من الملفات)، التي يكون هناك احتمال كبير لاستخدامها بواسطة المتطفلين للضرر بكمبيوتر المستخدم أو بيانات المستخدم، إلى Kaspersky Lab لإجراء فحوصات إضافية لها.

يحمي Kaspersky Lab جميع البيانات المستلمة كما هو مطلوب بواسطة القوانين المعمول بها. تستخدم Kaspersky Lab جميع المعلومات المستلمة فقط كإحصائيات كلية. يتم بشكل تلقائي الحصول على الإحصائيات الكلية من المعلومات المصدرية المستلمة، وهي لا تتضمن أي بيانات شخصية أو معلومات سرية أخرى. يتم تخزين المعلومات المصدرية بصيغة مشفرة، ويتم إتلافها مع تراكمها (مرتان كل عام). يتم تخزين الإحصائيات الكلية بشكل غير محدود.

شراء ترخيص

إذا قمت بتثبيت Kaspersky Total Security ولم تشتر ترخيصًا بعد، فيمكنك شراء ترخيص بعد التثبيت. عند شراء ترخيص، فستسلم رمز تفعيل يُستخدم لتفعيل التطبيق (راجع القسم "تفعيل التطبيق" على صفحة 32).

للحصول على ترخيص:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق رابط **الترخيص** لفتح نافذة **الترخيص**.
3. في النافذة التي ستفتح، انقر فوق زر **شراء رمز التفعيل**.

تفتح صفحة ويب Kaspersky Lab eStore أو شركة شركاء حيث يمكنك شراء ترخيص من عليها.

تفعيل التطبيق

للاستفادة من مزايا التطبيق وخدماته الإضافية، يجب عليك تفعيله.

إذا لم تقم بتفعيل التطبيق أثناء التثبيت، يمكنك تنفيذ هذا الأمر لاحقًا. سيتم تذكيرك بالحاجة إلى تفعيل التطبيق من خلال رسائل Kaspersky Total Security التي تظهر في منطقة الإخطارات بشريط المهام.

لتفعيل Kaspersky Total Security:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من نافذة التطبيق الرئيسية، انقر فوق الرابط **أدخل رمز التفعيل**. سيتم فتح نافذة **التفعيل**.

3. من نافذة **التفعيل**، أدخل رمز التفعيل في حقل الإدخال، وانقر فوق زر **تفعيل**.

تم تقديم طلب تفعيل التطبيق.

4. أدخل بيانات تسجيل المستخدم.

بناءً على بنود الاستخدام، قد يطالبك التطبيق بتسجيل الدخول إلى مدخل My Kaspersky. إذا لم تكن مستخدمًا مسجلاً، فأكمل نموذج التسجيل للوصول إلى الميزات الإضافية.

يمكن للمستخدمين المسجلين تنفيذ الإجراءات التالية:

- الاتصال بالدعم الفني ومعمل الفيروسات.
- إدارة رموز التفعيل.
- تلقي معلومات حول التطبيقات الجديدة والعروض الخاصة من Kaspersky Lab.

هذه الخطوة متاحة في بعض إصدارات Kaspersky Total Security.

5. انقر فوق الزر **إنهاء** في النافذة **التفعيل** لإتمام إجراء التسجيل.

تجديد ترخيص

يمكنك تجديد ترخيص عندما يصبح على وشك الانتهاء. للقيام بذلك، يمكنك تحديد رمز تفعيل جديد دون الانتظار حتى تنتهي صلاحية الترخيص الحالي. عند انتهاء صلاحية الترخيص الحالي، يقوم Kaspersky Total Security بالتنشيط التلقائي باستخدام رمز التنشيط الإضافي.

لتحديد رمز تفعيل إضافي للتجديد التلقائي للترخيص:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق رابط **الترخيص** لفتح نافذة **الترخيص**.
3. في النافذة التي يتم فتحها في قسم **رمز التفعيل الجديد**، انقر فوق زر **أدخل رمز التفعيل**.
4. أدخل رمز التفعيل في الحقول المناسبة، وانقر فوق زر **إضافة**.

يرسل Kaspersky Total Security بعد ذلك البيانات إلى خادم تفعيل Kaspersky Lab للتحقق منها.

5. انقر فوق زر **إنهاء**.

سيتم عرض رمز التفعيل الجديد في نافذة **الترخيص**.

يتم تفعيل التطبيق تلقائيًا باستخدام رمز التفعيل الجديد عند انتهاء صلاحية الترخيص. يمكنك أيضًا تفعيل التطبيق يدويًا باستخدام رمز تفعيل جديد عن طريق النقر فوق الزر **التفعيل الآن**. يتوفر هذا الزر إذا لم يتم تفعيل التطبيق تلقائيًا. لا يتوفر هذا الزر قبل انتهاء صلاحية الترخيص.

إذا تم تطبيق رمز التفعيل الجديد الذي حددته على هذا الكمبيوتر أو كمبيوتر آخر، فإن تاريخ التفعيل لغرض تجديد الترخيص هو تاريخ التفعيل الأول باستخدام رمز التفعيل هذا.

إدارة إخطارات التطبيق

تبلغك الإخطارات التي تظهر في منطقة الإخطارات بشريط المهام بأحداث التطبيق التي تستدعي اهتمامك. ووفقًا لدرجة حرج الحدث، قد تتلقى الأنواع التالية من الإخطارات:

- تخبرك *الإخطارات الحرجة* بأحداث ذات أهمية بالغة لأمان الكمبيوتر، مثل اكتشاف كائن ضار أو نشاط خطر في نظام التشغيل. النوافذ المستخدمة للإخطارات الحرجة والرسائل المنبثقة حمراء اللون.
- تخبرك *الإخطارات المهمة* بأحداث قد تكون مهمة لأمان الكمبيوتر، مثل اكتشاف كائن محتمل إصابته أو نشاط مشكوك فيه بنظام التشغيل. النوافذ المستخدمة للإخطارات المهمة والرسائل المنبثقة صفراء اللون.
- تخبرك *إخطارات المعلومات* بأحداث لا تمثل أهمية بالغة لأمان الكمبيوتر. النوافذ المستخدمة لإخطارات المعلومات والرسائل المنبثقة خضراء اللون.

في حالة عرض إخطار على الشاشة، ينبغي عليك اختيار أحد الخيارات التي يوفرها الإخطار. الخيار المثالي هو الموصى به كالخيار الافتراضي من قِبل خبراء Kaspersky Lab. يمكن إغلاف الإخطار تلقائيًا عند إعادة تشغيل الكمبيوتر، أو عند إنهاء تطبيق Kaspersky Total Security، أو في وضع "الاستعداد مع الاتصال" في نظام التشغيل Windows 8. عند غلق إخطار تلقائيًا، يقوم Kaspersky Total Security بتنفيذ الإجراء الافتراضي الموصى به.

لا يتم عرض الإخطارات خلال أول ساعة من تشغيل التطبيق في حالة قيامك بشراء كمبيوتر مُثبَّت عليه Kaspersky Total Security مسبقًا (توزيع OEM). اكتشفت عمليات التطبيق كائنات وفقًا للإجراءات الموصى بها. يتم حفظ نتائج هذه المعالجة في تقرير.

تقييم حالة حماية الكمبيوتر وحل مشكلات الأمان

يتم تمثيل المشكلات المتعلقة بحماية الكمبيوتر من خلال مؤشر يوجد في الجزء العلوي لنافذة التطبيق الرئيسية. يشير اللون الأخضر إلى أن الكمبيوتر الخاص بك محمي. يشير اللون الأصفر إلى وجود مشكلات في الحماية، بينما يشير اللون الأحمر إلى أن أمان الكمبيوتر الخاص بك في خطر شديد. ويوصى بالمعالجة الفورية للتغلب على المشكلات وتهديدات الأمان.

يؤدي النقر فوق المؤشر في نافذة التطبيق الرئيسية إلى فتح النافذة **مركز الإخطارات** (راجع الشكل التالي)، والتي تحتوي على معلومات تفصيلية حول حالة حماية الكمبيوتر واقتراحات لكيفية حل المشكلات والتهديدات المكتشفة.



الشكل *1*. نافذة مركز الإخطارات

يتم تجميع مشكلات الحماية حسب الفئات. ولكل مشكلة، يتم عرض قائمة تضم الإجراءات التي يمكنك اتخاذها لحل تلك المشكلة.

تحديث قواعد البيانات ووحدات البرنامج النمطية

بشكل افتراضي، يبحث Kaspersky Total Security تلقائيًا عن التحديثات على خوادم Kaspersky Lab الخاصة بالتحديث. إذا كان الخادم به مجموعة من التحديثات الجديدة، فسيقوم Kaspersky Total Security بتنزيلها وتثبيتها بشكل غير مرئي في الخلفية. يمكنك تشغيل أحد تحديثات Kaspersky Total Security يدويًا في أي وقت من نافذة التطبيق الرئيسية أو من القائمة السياقية لأيقونة التطبيق الموجودة في منطقة الإخطارات بشريط المهام.

لتنزيل تحديثات من خوادم تحديث Kaspersky Lab، يجب أن تكون متصلاً بالإنترنت.

مع نظام التشغيل Microsoft Windows 8، لا يتم تنزيل التحديثات في حالة إجراء اتصال واسع النطاق بالإنترنت وفرض حد على حركة نقل البيانات على هذا النوع من الاتصال. ولتنزيل التحديثات، يجب تعطيل الحد يدويًا في نافذة إعدادات التطبيق في قسم **الشبكة** الفرعي.

لتشغيل تحديث من القائمة السياقية لرمز التطبيق الموجود في منطقة الإخطارات بشريط المهام:

من القائمة السياقية لرمز التطبيق، حدد **تحديث**.

لتشغيل تحديث من نافذة لتطبيق الرئيسية:

1. افتح نافذة التطبيق الرئيسية وانقر فوق الزر **تحديث**.

   تعرض النافذة القسم **تحديث**.

2. في القسم **تحديث**، انقر فوق الزر **تشغيل التحديث**.

فحص الكمبيوتر

يقدم هذا القسم معلومات حول كيفية فحص الكمبيوتر الخاص بك لاكتشاف الفيروسات والتهديدات الأخرى.

في هذا القسم

فحص كامل

أثناء الفحص الكامل، يفحص Kaspersky Total Security الكائنات التالية بشكل افتراضي:

- ذاكرة النظام
- الكائنات التي يتم تحميلها عند بدء نظام التشغيل
- المخزن
- محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة

نوصي بتشغيل فحص كامل فور تثبيت Kaspersky Total Security على الكمبيوتر.

لبدء فحص كامل:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الزر **فحص**.

   يتم فتح نافذة **فحص**.
3. في نافذة **فحص**، حدد القسم **فحص كامل**.
4. في قسم **فحص كامل**، انقر فوق الزر **تشغيل الفحص**.

   يبدأ Kaspersky Total Security الفحص الكامل للكمبيوتر.

فحص مخصص

يتيح لك الفحص المخصص فحص ملف أو مجلد أو محرك أقراص لمعرفة الفيروسات والتهديدات الأخرى.

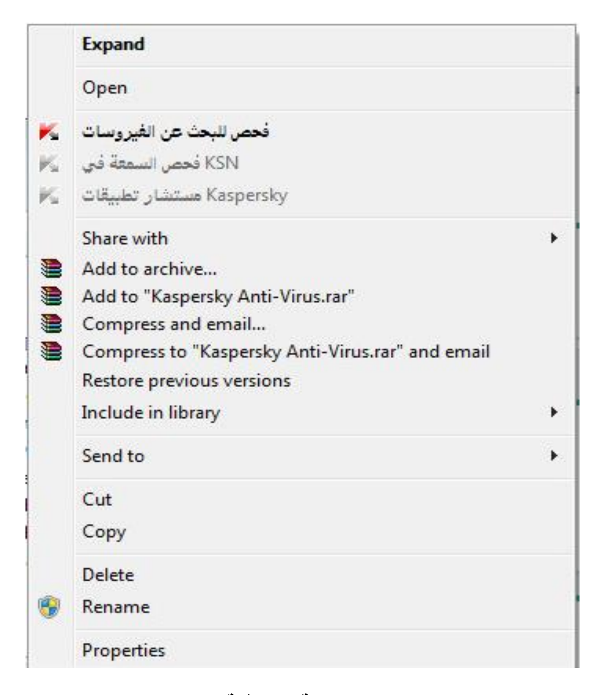
يمكنك بدء الفحص المخصص بالطرق التالية:

- من قائمة السياق الخاصة بالكائن؛

- من نافذة التطبيق الرئيسية،

لبدء فحص مخصص من القائمة السياقية لكائن:

1. افتح Microsoft Windows Explorer، وانتقل إلى المجلد الذي يحتوي على الكائن المراد فحصه.
2. انقر بزر الماوس الأيمن لفتح قائمة السياق الخاصة بالكائن (انظر الشكل التالي) وحدد **فحص للبحث عن الفيروسات**.



الشكل *2*. **القائمة السياقية للكائن**

لبدء تشغيل الفحص المخصص من نافذة التطبيق الرئيسية:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الزر **فحص**.

   يتم فتح نافذة **فحص**.
3. في نافذة **فحص**، حدد القسم **فحص مخصص**.
4. حدد الكائنات المطلوب فحصها بإحدى الطرق التالية:
   - اسحب الكائنات إلى النافذة **فحص مخصص**.
   - انقر فوق الزر **إضافة**، وحدد كائنًا في نافذة تحديد الملف أو المجلد التي يتم فتحها.
5. انقر فوق الزر **تشغيل الفحص**.

فحص سريع

أثناء الفحص السريع، يفحص Kaspersky Total Security الكائنات التالية بشكل افتراضي:

- الكائنات التي يتم تحميلها عند بدء نظام التشغيل

- ذاكرة النظام
- مقاطع بدء التشغيل بالقرص

لبدء فحص سريع:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الزر **فحص**.

   يتم فتح نافذة **فحص**.
3. في نافذة **فحص**، حدد القسم **فحص سريع**.
4. في قسم **فحص سريع**، انقر فوق الزر **تشغيل الفحص**.

يبدأ Kaspersky Total Security الفحص السريع للكمبيوتر.

فحص الملفات المحتمل إصابتها

إذا كنت تشك في إصابة ملف، فقم بفحصه باستخدام Kaspersky Total Security (راجع القسم "فحص مخصص" على صفحة 37).

إذا أكمل التطبيق الفحص وأبلغك أن الملف آمن على الرغم من أنك كنت تشك فيه، فيمكنك إرسال هذا الملف إلى *معمل الفيروسات*. يقوم خبراء معمل الفيروسات بفحص الملف. في حالة اكتشاف أنه مصاب بفيروس أو يشكل تهديدًا مختلفًا، فإنهم يقومون بإضافة وصف الفيروس الجديد إلى قواعد البيانات. يقوم التطبيق بتنزيل قواعد البيانات أثناء تحديث قواعد البيانات ووحدات التطبيق (راجع القسم "تحديث قواعد البيانات ووحدات البرنامج" على صفحة 36).

لإرسال ملف إلى "معمل الفيروسات":

1. انتقل إلى صفحة الطلب معمل الفيروسات (http://support.kaspersky.com/virlab/helpdesk.html).
2. اتبع التعليمات الواردة في هذه الصفحة لإرسال الطلب الخاص بك.

فحص الثغرات الأمنية

الثغرات الأمنية هي أجزاء غير محمية في رمز البرنامج قد يستخدمها المتطفلون عمدًا في أغراض تخصهم، مثل نسخ البيانات المستخدمة بواسطة التطبيقات ـ ذات الرموز غير المحمية. ويساعد فحص الكمبيوتر بحثًا عن الثغرات الأمنية في اكتشاف أي نقاط ضعف من هذا القبيل في حماية الكمبيوتر. وننصحك بمعالجة أي ثغرات أمنية يتم العثور عليها.

لبدء فحص ثغرات أمنية:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.
3. في الجزء الأيمن من نافذة **الأدوات**، انقر فوق الرابط **فحص الثغرات الأمنية** لفتح نافذة **فحص الثغرات الأمنية**.
4. في نافذة **فحص الثغرات الأمنية**، انقر فوق الزر **تشغيل الفحص**.

يبدأ Kaspersky Total Security فحص الكمبيوتر بحثًا عن ثغرات أمنية.

استعادة كائن تم حذفه أو تنظيفه بواسطة التطبيق

توصي شركة Kaspersky Lab المستخدم بتجنب استعادة الكائنات التي تم حذفها وتنظيفها حيث إنها يمكن أن تشكل تهديدًا على جهاز الكمبيوتر.

لاستعادة كائن تم حذفه أو تنظيفه، يمكنك استخدام النسخة الاحتياطية منه، والتي تم إنشاؤها بواسطة التطبيق أثناء فحص الكائن.

لا يقوم Kaspersky Total Security بتنظيف تطبيقات "متجر Windows". وإذا أوضحت نتائج الفحص أن التطبيق خطر، فسيتم حذفه من الكمبيوتر.

عند حذف أحد تطبيقات "متجر Windows"، لا يقوم Kaspersky Total Security بإنشاء نسخة احتياطية منه. ولاستعادة مثل هذه الكائنات، يجب عليك استخدام أدوات الاسترداد المدمجة مع نظام التشغيل (لمعرفة المعلومات التفصيلية، راجع الوثائق الخاصة بنظام التشغيل المُثبَّت على الكمبيوتر)، أو قم بتحديث التطبيقات عن طريق "متجر Windows".

لاستعادة ملف تم حذفه أو تنظيفه بواسطة التطبيق:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.
3. في الجزء الأيمن من نافذة **الأدوات**، انقر فوق الرابط **العزل** لفتح نافذة **العزل**.
4. في نافذة **العزل** التي يتم فتحها، حدد الملف المطلوب من القائمة، وانقر فوق زر **استعادة**.

استكشاف أخطاء نظام التشغيل وإصلاحها بعد الإصابة

يقدم هذا القسم معلومات حول كيفية استعادة نظام التشغيل بعد إصابته بالفيروسات.

في هذا القسم

استعادة نظام التشغيل بعد الإصابة

إذا كنت تشك في أن نظام تشغيل الكمبيوتر تعرض للتلف أو التعديل نتيجة نشاط برمجيات ضارة أو عطل في النظام، فاستخدم *معالج استكشاف أخطاء Microsoft Windows وإصلاحها*، الذي يمسح النظام من أي آثار للكائنات الضارة. وتوصي شركة Kaspersky Lab المستخدم بتشغيل المعالج بعد أن يتم تنظيف الكمبيوتر، وذلك للتأكد من التخلص من جميع التهديدات وإصلاح الضرر الناجم عن الإصابة.

يتحقق المعالج مما إذا كان هناك أي تغييرات في النظام، والتي قد تشمل منع الوصول إلى الشبكة، وتغيير امتدادات أسماء الملفات للتنسيقات المعروفة، وتأمين لوحة التحكم، وما إلى ذلك. وتوجد أسباب مختلفة لهذه الأنواع المختلفة من الأضرار. وقد تتضمن هذه الأسباب نشاط البرامج الضارة، أو تكوين النظام بشكل خاطئ، أو أعطال النظام، أو تعطل تطبيقات تحسين النظام.

بعد اكتمال المراجعة، يقوم "المعالج" بتحليل المعلومات لتقييم ما إذا كان هناك تلف بالنظام يتطلب الاهتمام به في الحال. وبناءً على المراجعة، ينشئ "المعالج" قائمة بالإجراءات اللازمة لمعالجة التلف. ويقوم المعالج بتصنيف هذه الإجراءات إلى فئات بناءً على درجة خطورة المشكلات المكتشفة.

استكشاف أخطاء نظام التشغيل وإصلاحها عن طريق استخدام معالج استكشاف أخطاء MICROSOFT WINDOWS وإصلاحها

لتشغيل "معالج استكشاف أخطاء Microsoft Windows وإصلاحها":

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.
3. في الجزء الأيمن من نافذة **الأدوات**، انقر فوق الرابط **استكشاف مشكلات Microsoft Windows وإصلاحها** لتشغيل معالج استكشاف أخطاء Microsoft Windows وإصلاحها.

   يتم فتح نافذة "معالج استكشاف أخطاء Microsoft Windows وإصلاحها".

يتكون "المعالج" من سلسلة من الصفحات (الخطوات) التي يمكنك التنقل بينها بالنقر فوق الزرين **رجوع** و**التالي**. لإغلاق "المعالج" بعد انتهائه، انقر فوق الزر **إنهاء**. لإيقاف المعالج في أي مرحلة، انقر الزر **إلغاء**.

دعنا نقوم بمراجعة خطوات المعالج بقدر أكبر من التفصيل.

الخطوة 1. بدء استعادة نظام التشغيل

تأكد من تحديد خيار المعالج **البحث عن المشكلات الناتجة عن نشاط البرمجيات الخبيثة** وانقر الزر **التالي**.

الخطوة 2. البحث عن المشكلات

يبحث "المعالج" عن المشكلات والتلف التي ينبغي معالجتها. وبمجرد أن ينتهي البحث، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

الخطوة 3. تحديد إجراءات استكشاف الأخطاء وإصلاحها

يتم تجميع جميع حالات التلف المكتشفة في الخطوة السابقة حسب نوع الخطر الذي تشكله. وبالنسبة لكل مجموعة من حالات التلف، توصي Kaspersky Lab بمجموعة من الإجراءات لمعالجة التلف. وتوجد ثلاث مجموعات من الإجراءات:

- *إجراءات موصى بها بشدة* وهي الإجراءات التي تقضي على المشكلات التي تمثل خطراً شديداً على الأمان. وينصح بتنفيذ جميع الإجراءات في هذه المجموعة.
- *إجراءات موصى بها* وتهدف إلى معالجة الضرر الذي يمثل تهديدًا. وينصح بتنفيذ جميع الإجراءات في هذه المجموعة أيضًا.
- *إجراءات إضافية* وهي الإجراءات التي تقوم بإصلاح تلف النظام الذي لا يمثل تهديداً حالياً، إلا أنه قد يمثل خطرًا على أمان الكمبيوتر في المستقبل.

لعرض الإجراءات داخل مجموعة ما، انقر فوق علامة الزائد + على يمين اسم المجموعة.

لجعل المعالج يقوم بتنفيذ إجراء معين، حدد خانة الاختيار الموجودة على يمين الإجراء المعني. وافتراضيًا، ينفذ المعالج جميع الإجراءات المستحسنة والمستحسنة بشدة. إذا كنت لا ترغب في تنفيذ إجراء معين، فقم بإلغاء تحديد خانة الاختيار المجاورة له.

يوصى بشدة بعدم إلغاء تحديد خانات الاختيار المحددة بشكل افتراضي لأن القيام بذلك سيجعل الكمبيوتر عرضة للتهديدات.

بعد تحديد مجموعة الإجراءات التي سيقوم المعالج بتنفيذها، انقر فوق زر **التالي**.

الخطوة 4. إصلاح المشكلات

سينفذ المعالج الإجراءات المحددة أثناء الخطوة السابقة. قد يستغرق إصلاح المشكلات بعض الوقت. عند اكتمال استكشاف الأخطاء وإصلاحها، يتابع "المعالج" تلقائيًا إلى الخطوة التالية.

الخطوة 5. اكتمال المعالج

انقر الزر **إنهاء** لإغلاق المعالج.

حماية البريد الإلكتروني

يقدم هذا القسم معلومات حول كيفية حماية البريد الإلكتروني من البريد الإلكتروني غير المرغوب فيه لاكتشاف الفيروسات والتهديدات الأخرى.

في هذا القسم

تكوين مكافحة فيروسات البريد

يتيح Kaspersky Total Security فحص رسائل البريد الإلكتروني بحثًا عن الكائنات الخطرة باستخدام المكون "مكافحة فيروسات البريد". يبدأ تشغيل مكون مكافحة فيروسات البريد عند بدء تشغيل نظام التشغيل ويبقى في ذاكرة الوصول العشوائي (RAM) بشكل دائم ليقوم بفحص كل رسائل البريد الإلكتروني التي يتم إرسالها أو تلقيها عبر بروتوكولات POP3، وSMTP، وIMAP، وNNTP، إلى جانب الاتصالات المشفرة (SSL) عبر بروتوكولات POP3، وSMTP، وIMAP.

وبشكل افتراضي، يفحص مكون مكافحة فيروسات البريد كلاً من الرسائل الواردة والصادرة. إذا تطلب الأمر، فيمكنك تمكين فحص الرسائل الواردة فقط.

لتكوين المكون "مكافحة فيروسات البريد":

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الإعدادات**.
3. في الجزء الأيسر من النافذة، في القسم **الحماية**، حدد المكون **مكافحة فيروسات البريد**.

   يتم عرض إعدادات المكون "مكافحة فيروسات البريد" في النافذة.
4. تأكد من تمكين زر التبديل الموجود في الجزء العلوي من النافذة، والذي يقوم بتمكين / تعطيل المكون "مكافحة فيروسات البريد".
5. حدد مستوى الأمان:
   - **مستحسن**. في حالة تحديد مستوى الأمان هذا، يفحص المكون "مكافحة فيروسات البريد" الرسائل الواردة والصادرة، كما أنه يفحص الأرشيفات المرفقة.
   - **منخفض**. في حالة تحديد مستوى الأمان هذا، يفحص المكون "مكافحة فيروسات البريد" الرسائل الواردة فقط دون فحص الأرشيفات المرفقة.
   - **مرتفع**. في حالة تحديد مستوى الأمان هذا، يفحص المكون "مكافحة فيروسات البريد" الرسائل الواردة والصادرة، كما أنه يفحص الأرشيفات المرفقة. عند تحديد مستوى أمان مرتفع، يتم تمكين تحليل مساعد على الاكتشاف عميق.
6. في القائمة المنسدلة **إجراء عند اكتشاف تهديد**، حدد إجراءً ينبغي على المكون "مكافحة فيروسات البريد" القيام به عند اكتشاف كائن مصاب (مثل إجراء التنظيف).

في حالة عدم اكتشاف أي تهديدات في رسالة البريد الإلكتروني، أو في حالة تنظيف كل الكائنات المصابة بنجاح، تصبح الرسالة متاحة للوصول اللاحق. إذا فشل المكون في تنظيف كائن مصاب، فسيعيد المكون "مكافحة فيروسات البريد" تسمية الكائن أو يحذفه من الرسالة، ويضيف إخطارًا إلى سطر عنوان الرسالة يفيد بأنه تمت معالجة الرسالة بواسطة Kaspersky Total Security. قبل حذف كائن، يقوم Kaspersky Total Security بإنشاء نسخة احتياطية منه ووضع هذه النسخة في العزل (انظر قسم "استعادة كائن تم حذفه أو تنظيفه بواسطة التطبيق" في صفحة 40).

منع البريد الإلكتروني غير المرغوب به (البريد العشوائي)

إذا كنت تتلقى كميات كبيرة من الرسائل غير المرغوب فيها (العشوائية)، فقم بتمكين المكون "مكافحة البريد الإلكتروني غير المرغوب فيه" وتعيين مستوى الأمان الموصى به لها.

لتمكين مكافحة البريد الإلكتروني غير المرغوب فيه وتحديد مستوى الأمان المستحسن:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الإعدادات**. انتقل إلى قسم **الإعدادات**.
3. في الجزء الأيمن من النافذة، حدد القسم **الحماية**.
4. في الجزء الأيمن من القسم **الحماية**، حدد المكون **مكافحة البريد الإلكتروني غير المرغوب فيه**.

   تعرض النافذة إعدادات "مكافحة البريد الإلكتروني غير المرغوب فيه".
5. في الجزء الأيسر من النافذة، قم بتمكين "مكافحة البريد الإلكتروني غير المرغوب فيه" باستخدام مفتاح التبديل.
6. في القسم **مستوى الأمان**، تأكد من تعيين مستوى الأمان **الموصى به**.

حماية البيانات الخاصة على الإنترنت

يوفر هذا القسم معلومات حول كيفية جعل استعراض الإنترنت آمنًا وحماية بياناتك من السرقة.

في هذا القسم

حول حماية البيانات الخاصة على الإنترنت

يساعدك Kaspersky Total Security على حماية البيانات الشخصية من السرقة:

- كلمات المرور وأسماء المستخدم وبيانات التسجيل الأخرى
- أرقام الحسابات وأرقام البطاقات البنكية

يشتمل Kaspersky Total Security على مكونات وأدوات تتيح لك حماية بياناتك الشخصية ضد محاولات السرقة التي يقوم بها المجرمون الذين يستخدمون طرقًا مثل الاحتيال واعتراض البيانات المدخلة على لوحة المفاتيح.

يتم تقديم الحماية ضد الاحتيال بواسطة مكون "مكافحة الاحتيال"، والتي يتم تنفيذها في مكون "مكافحة فيروسات الويب" ومكون "مكافحة البريد الإلكتروني غير المرغوب فيه" ومكون "مكافحة فيروسات المراسلة الفورية". وتمكن هذه المكونات من ضمان توفير حماية شاملة ضد الاحتيال.

يتم توفير الحماية من اعتراض البيانات المدخلة على لوحة المفاتيح بواسطة "لوحة المفاتيح الظاهرية" والإدخال الآمن للوحة المفاتيح.

يمسح معالج منظف الخصوص الكمبيوتر من كل المعلومات حول أنشطة المستخدم.

تحمي الخدمات النقدية الآمنة البيانات عند استخدام الخدمات البنكية على الإنترنت والتسوق من المتاجر عبر الإنترنت.

يتم تقديم الحماية لنقل البيانات الخاصة عبر الإنترنت بواسطة أحد أدوات الرقابة الأسرية (انظر القسم "استخدام الرقابة الأسرية" على صفحة 59).

حول لوحة المفاتيح الظاهرية

عند استخدام الإنترنت، تحتاج كثيرًا إلى إدخال بياناتك الشخصية أو اسم المستخدم وكلمة المرور خاصتك. ويحدث هذا، على سبيل المثال، أثناء تسجيل حساب على مواقع الويب، أو أثناء التسوق عبر الويب، أو إجراء معاملات بنكية على الإنترنت.

هناك خطر من اعتراض هذه المعلومات الشخصية عن طريق معترضي لوحات المفاتيح، أو برامج رصد لوحة المفاتيح، وهي عبارة عن برامج تقوم بتسجيل ضغطات لوحة المفاتيح المادية. تمنع لوحة المفاتيح الظاهرية اعتراض البيانات المدخلة باستخدام لوحة المفاتيح.

وتستطيع الكثير من البرامج المصنفة كبرامج تجسس التقاط لقطات للشاشة، والتي يمكن نقلها بشكل تلقائي إلى دخيل لإجراء المزيد من التحليل ولسرقة البيانات الشخصية للمستخدم. تعمل لوحة المفاتيح الظاهرية على حماية البيانات الشخصية التي تم إدخالها من محاولات اعتراضها من خلال استخدام لقطات الشاشة.

تتضمن "لوحة المفاتيح الظاهرية" المزايا التالية:

- يمكنك النقر فوق أزرار "لوحة المفاتيح الظاهرية" باستخدام الماوس.
- بخلاف لوحات المفاتيح المادية، لا يمكن النقر فوق عدة مفاتيح في وقت واحد على "لوحة المفاتيح الظاهرية". لهذا فإن استخدام مجموعات المفاتيح (مثل **ALT+F4**) يتطلب النقر فوق المفتاح الأول (على سبيل المثال، **ALT**)، ثم المفتاح الثاني (على سبيل المثال، **F4**)، ثم المفتاح الأول مرة أخرى. تعمل النقرة الثانية فوق المفتاح بنفس الطريقة كما لو تركت المفتاح على لوحة مفاتيح مادية.
- يمكن تبديل لغة "لوحة المفاتيح الظاهرية" باستخدام نفس الاختصار الذي توفره إعدادات نظام التشغيل الخاص بلوحة المفاتيح المادية. للقيام بذلك، انقر بزر الماوس الأيمن فوق المفتاح الآخر (على سبيل المثال، إذا تم تكوين الاختصار **LEFT ALT+SHIFT** في إعدادات نظام التشغيل لتبديل لغة لوحة المفاتيح، فانقر بزر الماوس الأيسر فوق المفتاح **LEFT ALT** وثم انقر بزر الماوس الأيمن فوق المفتاح **SHIFT**).

لضمان حماية البيانات التي تم إدخالها عبر لوحة المفاتيح الظاهرية، قم بإعادة تشغيل الكمبيوتر بعد تثبيت Kaspersky Total Security.

ينطوي استخدام لوحة المفاتيح الظاهرية على القيود التالية:

- تمنع لوحة المفاتيح الظاهرية اعتراض البيانات الشخصية فقط عند استخدامها مع مستعرضات Microsoft Internet Explorer أو Mozilla Firefox أو Google Chrome. عند الاستخدام مع مستعرضات أخرى، لا تحمي "لوحة المفاتيح الظاهرية" البيانات الشخصية التي يتم إدخالها ضد الاعتراض.
- لوحة المفاتيح الظاهرية غير متاحة للمستعرض Microsoft Internet Explorer 10 و11 بنمط واجهة المستخدم الجديدة أو للمستعرض Microsoft Internet Explorer 10 و11 في حالة تحديد خانة الاختيار **تمكين الوضع المحمي المحسّن** في إعدادات المستعرض. في هذه الحالة، نوصي بفتح لوحة المفاتيح الظاهرية من واجهة Kaspersky Total Security.
- لا تستطيع لوحة المفاتيح الظاهرية حماية بياناتك الشخصية إذا تعرض الموقع، الذي يطلب إدخال هذه البيانات، لهجوم القراصنة، حيث إنه في هذه الحالة سيتم الحصول على المعلومات مباشرة عن طريق الدخلاء من موقع الويب.
- لا تمنع لوحة المفاتيح الظاهرية لقطات الشاشة التي تم إجراؤها باستخدام مفتاح **PRINT SCREEN** ومجموعات المفاتيح الأخرى المحددة في إعدادات نظام التشغيل.
- عند تشغيل لوحة المفاتيح الظاهرية تتوقف ميزة AutoComplete بمستعرض Microsoft Internet Explorer عن العمل، نظرًا لأن تنفيذ مخطط الإدخال التلقائي قد يسمح للمجرمين بمقاطعة البيانات.
- في بعض المستعرضات (مثل Google Chrome)، قد لا تعمل حماية إدخال البيانات لبعض أنواع البيانات (مثل عناوين البريد الإلكتروني أو الأرقام).

توضح القائمة السابقة القيود الأساسية على وظائف حماية إدخال البيانات. وتوجد قائمة كاملة بالقيود في مقال على موقع ويب الدعم الفني لـ Kaspersky Lab http://support.kaspersky.com/11048.

بدء لوحة المفاتيح الظاهرية.

يمكنك فتح لوحة المفاتيح الظاهرية بالطرق التالية:

- من القائمة السياقية الخاصة برمز التطبيق الموجود في منطقة إخطارات شريط المهام؛

- من نافذة التطبيق الرئيسية،
- من نافذة Microsoft Internet Explorer أو Mozilla Firefox أو Google Chrome عن طريق النقر فوق رمز الوصول السريع إلى لوحة المفاتيح الظاهرية

> يمكنك تكوين عرض رمز بدء التشغيل السريع في حقول الإدخال على مواقع الويب.
>
> عند استخدام "لوحة المفاتيح الظاهرية"، يقوم Kaspersky Total Security بتعطيل خيار الملء التلقائي لحقول الإدخال على مواقع الويب.

- من خلال الضغط على مجموعة من مفاتيح لوحة المفاتيح.

➡ *لفتح "لوحة المفاتيح الظاهرية" من القائمة السياقية لرمز التطبيق في منطقة الإخطارات بشريط المهام:*

في القائمة السياقية لرمز التطبيق (انظر الشكل التالي)، حدد **أدوات**□**لوحة المفاتيح الظاهرية**



الشكل 3. القائمة السياقية لبرنامج *Kaspersky Total Security*

➡ *لفتح "لوحة المفاتيح الظاهرية" من نافذة التطبيق الرئيسية:*

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.
3. في الجزء الأيمن من نافذة **الأدوات**، انقر فوق الرابط **لوحة المفاتيح الظاهرية** لفتح لوحة المفاتيح الظاهرية.

➡ *لفتح لوحة المفاتيح الظاهرية من نافذة المستعرض:*

انقر فوق الزر [K] **لوحة المفاتيح الظاهرية** الموجود في شريط أدوات Microsoft Internet Explorer، أو Mozilla Firefox، أو Google Chrome.

➡ *لفتح "لوحة المفاتيح الظاهرية" باستخدام لوحة المفاتيح المادية:*

اضغط الاختصار **CTRL+ALT+SHIFT+P**.

➡ *لتكوين عرض رمز بدء التشغيل السريع للوحة المفاتيح الظاهرية في حقول الإدخال على مواقع الويب:*

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الإعدادات**.
3. في نافذة **الإعدادات** التي يتم فتحها، في قسم **إضافي**، حدد القسم الفرعي **إدخال البيانات الآمن**.

تعرض النافذة إعدادات إدخال البيانات الآمن.

4. في لزم الأمر، فمن القسم **لوحة المفاتيح الظاهرية**، حدد خانة الاختيار **افتح لوحة المفاتيح الظاهرية عن طريق كتابة CTRL+ALT+SHIFT+P**.
5. إذا كنت تريد عرض أيقونة التشغيل السريع للوحة المفاتيح الظاهرية في حقول الإدخال، فحدد خانة الاختيار **إظهار أيقونة التشغيل السريع في حقول إدخال البيانات**.
6. إذا كنت تريد عرض رمز التشغيل السريع للوحة المفاتيح الظاهرية فقط عند فتح مواقع ويب معينة:
   a. في القسم **لوحة المفاتيح الظاهرية**، انقر فوق الرابط **تحرير الفئات** لفتح نافذة **إعدادات إدخال البيانات الآمن**.
   b. حدد خانات اختيار فئات مواقع الويب التي تريد عرض رمز التشغيل السريع عليها في حقول الإدخال.

   سيتم عرض رمز التشغيل السريع للوحة المفاتيح الظاهرية عند الوصول إلى موقع ويب ينتمي إلى أي من الفئات المحددة.

   c. إذا كنت تريد تمكين عرض رمز التشغيل السريع للوحة المفاتيح الظاهرية على موقع ويب معين أو تعطيل عرضها:
      a. انقر فوق الرابط **تكوين الاستثناءات** لفتح نافذة **استثناءات لوحة المفاتيح الظاهرية**.
      b. في الجزء السفلي من النافذة، انقر فوق زر **إضافة**.

      يتم فتح نافذة لإضافة استثناء للوحة المفاتيح الظاهرية.

      c. في حقل **قناع عنوان موقع الويب** أدخل عنوان الويب لموقع ويب.
      d. إذا كنت تريد عرض رمز بدء التشغيل السريع للوحة المفاتيح الظاهرية (أو عدم عرضها) على صفحة ويب معينة فقط، فمن القسم **النطاق**، حدد **تطبيق على الصفحة المحددة**.
      e. في القسم **رمز لوحة المفاتيح الظاهرية**، حدد ما إذا كان ينبغي عرض رمز التشغيل السريع للوحة المفاتيح الظاهرية على صفحة الويب المحددة أم لا.
      f. انقر فوق الزر **إضافة**.

      يظهر موقع الويب المحدد في القائمة الموجودة في النافذة **استثناءات لوحة المفاتيح الظاهرية**.

عند الوصول إلى موقع الويب المحدد، سيتم عرض رمز التشغيل السريع للوحة المفاتيح الظاهرية وفقًا للإعدادات المحددة.

حماية البيانات التي تم إدخالها على لوحة مفاتيح الكمبيوتر

تسمح حماية إدخال البيانات على لوحة مفاتيح الكمبيوتر بتجنب اعتراض البيانات المدخلة بواسطة لوحة المفاتيح.

يحتوي الإدخال الآمن للوحة المفاتيح على القيود التالية:

- تتوافر حماية إدخال البيانات بواسطة لوحة مفاتيح الكمبيوتر في مستعرضات Microsoft Internet Explorer و Mozilla Firefox و Google Chrome فقط. عند استخدام مستعرضات الويب الأخرى، لا تتم حماية البيانات المدخلة من لوحة مفاتيح الكمبيوتر من الاعتراض.
- لا يتوفر الإدخال الآمن للوحة المفاتيح في Microsoft Internet Explorer من متجر Windows.
- لا تقوم حماية إدخال البيانات بواسطة لوحة مفاتيح الكمبيوتر بحماية البيانات الشخصية إذا كان موقع الويب الذي يطالب بإدخال تلك البيانات قد تعرض للقرصنة، لأنه في تلك الحالة سيحصل الدخلاء على المعلومات مباشرة من موقع الويب.
- في بعض المستعرضات (مثل Google Chrome)، قد لا تعمل حماية إدخال البيانات لبعض أنواع البيانات (مثل عناوين البريد الإلكتروني أو الأرقام).

توضح القائمة السابقة القيود الأساسية على وظائف حماية إدخال البيانات. وتوجد قائمة كاملة بالقيود في مقال على موقع ويب الدعم الفني لـ Kaspersky Lab .http://support.kaspersky.com/11048

يمكنك تكوين حماية إدخال البيانات من لوحة مفاتيح الكمبيوتر على مواقع الويب المختلفة. بعد تكوين حماية إدخال البيانات من لوحة مفاتيح الكمبيوتر، ليس عليك اتخاذ أي إجراءات إضافية عند إدخال البيانات.

لتكوين حماية إدخال البيانات من لوحة مفاتيح الكمبيوتر:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الإعدادات**. انتقل إلى قسم **الإعدادات**.
3. في القسم **إضافي**، حدد القسم الفرعي **إدخال البيانات الآمن**.

   تعرض النافذة إعدادات إدخال البيانات الآمن.
4. في الجزء السفلي من النافذة، في قسم **إدخال لوحة المفاتيح الآمن**، حدد خانة الاختيار **تمكين الإدخال الآمن للوحة المفاتيح**.
5. حدد نطاق حماية إدخال البيانات من لوحة المفاتيح المادية:
   a. افتح النافذة **إعدادات إدخال البيانات الآمن** بالنقر فوق الرابط **تحرير الفئات** في الجزء السفلي من القسم **إدخال لوحة المفاتيح الآمن**.
   b. حدد خانات الاختيار لفئات مواقع الويب التي تريد حماية البيانات عليها والتي تم إدخالها عبر لوحة المفاتيح.
   c. إذا كنت تريد تمكين حماية إدخال البيانات من لوحة المفاتيح على موقع ويب معين:
      a. افتح النافذة **استثناءات إدخال لوحة المفاتيح الآمن** بالنقر فوق الرابط **تكوين الاستثناءات**.
      b. في النافذة، انقر فوق الزر **إضافة**.

         يتم فتح نافذة لإضافة استثناء للإدخال الآمن للوحة المفاتيح.
      c. في النافذة التي يتم فتحها، في حقل **قناع عنوان موقع الويب**، أدخل عنوان موقع الويب.
      d. حدد أحد خيارات "إدخال البيانات الآمن" على موقع الويب هذا (**تطبيق على الصفحة المحددة** أو **تطبيق على موقع الويب بأكمله**).
      e. حدد إجراءً ليتم القيام به بواسطة "الإدخال الآمن للبيانات" على موقع الويب هذا (**حماية** أو **بدون حماية**).
      f. انقر فوق الزر **إضافة**.

   يظهر موقع الويب المحدد في القائمة الموجودة في النافذة **استثناءات إدخال لوحة المفاتيح الآمن**. عند الوصول إلى موقع الويب هذا، سيتم تفعيل ميزة "إدخال البيانات الآمن" لتعمل وفقًا للإعدادات التي حددتها.

تكوين إخطارات الثغرات الأمنية في شبكات Wi-Fi

عند الاتصال بشبكة Wi-Fi، قد تتم سرقة بياناتك السرية إذا لم تتم حماية هذه الشبكة جيدًا. يفحص Kaspersky Total Security شبكات Wi-Fi كل مرة تتصل بإحدى هذه الشبكات. إذا كانت شبكة Wi-Fi غير آمنة (على سبيل المثال، استخدام بروتوكول تشفير به ثغرة أمنية أو أن اسم شبكة Wi-Fi (SSID)شائع جدًا)، فيعرض التطبيق إخطارًا يطلعك بأنك على وشك الاتصال بشبكة Wi-Fi غير آمنة. انقر فوق الرابط في نافذة الإخطار للتعرف على كيفية استخدام شبكة Wi-Fi بشكل آمن.

لتكوين إخطارات الثغرات الأمنية على شبكات Wi-Fi:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الإعدادات**. انتقل إلى قسم **الإعدادات**.

3. في الجزء الأيمن من النافذة، حدد القسم **الحماية**.

4. في الجزء الأيسر من القسم **الحماية**، حدد القسم الفرعي **جدار الحماية**.

تعرض النافذة إعدادات المكون "جدار الحماية".

5. حدد خانة الاختيار **إخطار بالثغرات الأمنية في شبكات Wi-Fi** إذا تم إلغاء تحديدها. إذا كنت لا ترغب في تلقي إخطارات، فقم بإلغاء تحديد خانة الاختيار. يتم تحديد خانة الاختيار هذه بشكل افتراضي.

6. إذا تم تحديد خانة الاختيار **إخطار بالثغرات الأمنية في شبكات** Wi-Fi فيمكنك تحرير الإعدادات المتقدمة لعرض الإخطارات:

- حدد خانة الاختيار **منع وتحذير من الإرسال غير الآمن لكلمات المرور عبر الإنترنت** لمنع جميع عمليات إرسال كلمات المرور كنص غير مشفر عند تعبئة حقول **كلمة المرور** على الإنترنت. ويتم إلغاء تحديد خانة الاختيار هذه بشكل افتراضي.
- انقر فوق الرابط **استعادة الإخطارات المخفية** للتراجع عن القيم الافتراضية للإعدادات لعرض إخطارات حول عمليات إرسال كلمات المرور في نموذج غير مشفر. إذا قمت سابقًا بحظر عرض إخطارات حول إرسال كلمة المرور في نموذج غير مشفر، فسيتم استئناف عرض هذه الإخطارات.

حماية التعاملات المالية وعمليات الشراء عبر الإنترنت

لتوفير الحماية للبيانات السرية التي تقوم بإدخالها على مواقع الويب الخاصة بالبنوك وأنظمة السداد (مثل أرقام البطاقات البنكية وكلمات المرور الخاصة بالوصول إلى الخدمات البنكية عبر الإنترنت)، بالإضافة إلى منع سرقة الأموال عند السداد عبر الإنترنت، يطلب منك Kaspersky Total Security فتح مواقع الويب هذه في المستعرض المحمي.

المستعرض المحمي هو وضع تشغيل مستعرض خاص مصمم لحماية بياناتك عند الوصول إلى مواقع ويب البنوك أو أنظمة الدفع. يتم بدء المستعرض المحمي في بيئة معزولة لمنع التطبيقات الأخرى من إدخال رمزها في عملية المستعرض المحمي.

في وضع المستعرض المحمي، يوفر التطبيق حماية ضد أنواع التهديدات التالية:

- الوحدات النمطية غير الموثوق بها. يقوم التطبيق بإجراء فحص لمعرفة الوحدات النمطية غير الموثوق بها كل مرة تزور فيها موقع ويب بنك أو نظام دفع.
- فيروسات الجذر. يقوم التطبيق بالفحص لمعرفة فيروسات الجذر عند بدء تشغيل مستعرض محمي.
- ثغرات نظام التشغيل المعروفة. يقوم التطبيق بالفحص لمعرفة الثغرات الأمنية بنظام التشغيل عند بدء تشغيل مستعرض محمي.
- شهادات غير صالحة لمواقع ويب البنك وأنظمة الدفع. يتحقق التطبيق من الشهادات عند زيارة موقع ويب بنك أو نظام دفع. يتم إجراء الفحص ضد قاعدة بيانات الشهادات العرضة للخطر.

عند فتح موقع ويب في المستعرض المحمي، يظهر إطار على حدود نافذة المستعرض. يشير لون الإطار إلى حالة الحماية.

يمكن أن يعرض إطار نافذة المستعرض إشارات الألوان التالية:

- إطار أخضر. يشير إلى أن جميع الفحوصات قد تم إجراؤها بشكل ناجح. يمكنك الاستمرار في استخدام المستعرض المحمي.
- إطار أصفر. يشير إلى أن جميع الفحوصات تحتوي على مشكلات أمان ظاهرة تحتاج إلى حلها.

يمكن للتطبيق اكتشاف التهديدات ومشكلات الأمان التالية:

- الوحدة النمطية غير الموثوق بها. هناك حاجة لفحص الكمبيوتر وتنظيفه.
- Rootkit. هناك حاجة لفحص الكمبيوتر وتنظيفه.

- الثغرات الأمنية لنظام التشغيل. هناك حاجة لتثبيت تحديثات نظام التشغيل.
- شهادة غير صالحة لموقع ويب البنك أو نظام الدفع.

إذا لم تتخلص من التهديدات المكتشفة، فلا يتم ضمان جلسة اتصال موقع ويب البنك أو نظام الدفع.

قد يشير اللون الأصفر للإطار إلى أن المستعرض المحمي لا يمكن تشغيله نظرًا لقيود فنية. على سبيل المثال، يتم تشغيل hypervisor الخاص بطرف خارجي أو أن الكمبيوتر لا يدعم تقنية الأجهزة الظاهرية.

للاستخدام المناسب للمستعرض المحمي، تأكد من تفعيل المكونات الإضافية للخدمات النقدية الآمنة. يتم تفعيل المكونات الإضافية تلقائيًا في المستعرض عند إعادة تشغيله لأول مرة بعد تثبيت Kaspersky Total Security. في حالة عدم الخروج وتشغيل المستعرض مرة أخرى بعد تثبيت Kaspersky Total Security، لا يتم تفعيل المكونات الإضافية.

يحتوي التفعيل التلقائي للمكونات الإضافية على القيود التالية:

- يتم دمج المكونات الإضافية وتفعيلها فقط في المستعرضات المدعومة من التطبيق.

  تدعم المستعرضات التالية المكونات الإضافية للخدمات النقدية الآمنة:

  - Internet Explorer 8.0 و9.0 و10.0 و 11.0.

  لا يدعم التطبيق Internet Explorer 10 Modern UI style وInternet Explorer 11 Modern UI style.

  - Mozilla Firefox 19.x و20.x و21.x و22.x و23.x و24.x و25.x و26.x و27.x و28.x و29.x و30.x و31.x.
  - Google Chrome 33.x و34.x و35.x و و36.x.

  لا يتم تفعيل المكونات الإضافية لـ Google Chrome تلقائيًا إذا لم يتم إنشاء ملف بيانات المستخدم في المستعرض. لإنشاء ملف بيانات مستخدم، اخرج من المستعرض وقم بتشغيله مرة أخرى.

  عند التشغيل الأول لـ Google Chrome بعد تثبيت Kaspersky Total Security، يُطالبك مستعرض الويب بتثبيت امتداد يُسمى المكون الإضافي لـ Kaspersky Protection والذي يقوم بتفعيل المكونات الإضافية لمكون "الخدمات النقدية الآمنة". إذا رفضت تثبيت المكون الإضافي لحماية Kaspersky، فيمكنك تثبيته لاحقًا عن طريق النقر فوق هذا الرابط: http://support.kaspersky.com/interactive/google/en/kisplugin.

- عند تحديث المستعرض الخاص بك، يتم تفعيل المكونات الإضافية تلقائيًا فقط إذا كان الإصدار الجديد يدعم نفس طريقة تفعيل المكون الإضافي المتبعة مع الإصدار السابق. إذا كان الإصدار الجديد للمستعرض يدعم نفس طريقة تفعيل المكون الإضافي المتبعة مع الإصدار السابق، فيتم تفعيل المكونات الإضافية تلقائيًا.

إذا لم يتم تفعيل المكونات الإضافية تلقائيًا عند تشغيل المستعرض مرة أخرى، فتحتاج إلى تفعيلها يدويًا. يمكنك التحقق مما إذا كانت المكونات الإضافية مفعلة، وتفعيلها يدويًا في إعدادات المستعرض. يمكنك الرجوع إلى نظام التعليمات الخاص بالمستعرض الحالي للحصول على المزيد من التفاصيل حول تفعيل المكون الإضافي.

يمكنك تمكين أو تعطيل التفعيل التلقائي للمكونات الإضافية (انظر القسم "تمكين التفعيل التقائي للمكونات الإضافية الخاصة بالخدمات النقدية الآمنة" على صفحة 53) في نافذة إعدادات التطبيق.

لا يمكن تشغيل المستعرض المحمي في حالة عدم تحديد خانة الاختيار **تمكين الدفاع الذاتي** في القسم الفرعي **الدفاع الذاتي** بقسم **إعدادات إضافية** لنافذة إعدادات التطبيق.

في هذا القسم

تكوين الخدمات النقدية الآمنة

لتكوين الخدمات النقدية الآمنة:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **الإعدادات** للانتقال إلى قسم **الإعدادات**.
3. في الجزء الأيمن من النافذة، حدد القسم **الحماية**.
4. في الجزء الأيسر من القسم **الحماية**، حدد القسم الفرعي **الخدمات النقدية الآمنة**.

   تعرض النافذة إعدادات المكون "الخدمات النقدية الآمنة".
5. قم بتمكين "الخدمات النقدية الآمنة" بالنقر فوق مفتاح التبديل الموجود في الجزء العلوي من النافذة.
6. لتمكين الإخطارات بالثغرات الأمنية المكتشفة في نظام التشغيل قبل بدء تشغيل المستعرض المحمي، حدد خانة الاختيار **الإخطار بالثغرات الأمنية الموجودة في نظام التشغيل**.

تكوين الخدمات النقدية الآمنة لموقع ويب محدد

لتكوين الخدمات النقدية الآمنة لموقع ويب محدد:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الزر **الخدمات النقدية الآمنة**.

   سيتم فتح نافذة **الخدمات النقدية الآمنة**.
3. انقر فوق الزر **Add website to Safe Money**.

   يعرض الجزء الأيسر من النافذة حقولاً لإضافة تفاصيل موقع الويب.
4. في الحقل **موقع ويب للخدمات النقدية الآمنة**، أدخل عنوان الويب لموقع الويب الذي تريد فتحه في المستعرض المحمي.

يجب أن يكون عنوان موقع الويب مسبوقًا ببادئة بروتوكول //:tpsht والتي يتم استخدامها بشكل افتراضي بواسطة المستعرض المحمي.

5. عند الضرورة، في الحقل **الوصف** أدخل اسم أو وصف موقع الويب.
6. حدد الإجراء الذي تريد من المستعرض المحمي إجراءه عند فتح موقع الويب:
   - إذا كنت تريد فتح موقع الويب في المستعرض المحمي كل مرة تقوم فيها بزيارته، فحدد **تشغيل المستعرض المحمي**.
   - إذا كنت تريد أن يطالبك Kaspersky Total Security باتخاذ إجراء عند فتح موقع الويب، فحدد **المطالبة باتخاذ إجراء**.
   - إذا كنت تريد تعطيل "الخدمات النقدية الآمنة" لموقع الويب، فحدد **عدم تشغيل المستعرض المحمي**.
7. في الجزء الأيسر من النافذة، انقر فوق الزر **إضافة**.

سيتم عرض موقع الويب في القائمة الموجودة في الجزء الأيمن من النافذة.

تمكين التفعيل التلقائي للمكونات الإضافية للخدمات البنكية الآمنة

لتمكين تفعيل المكونات الإضافية للخدمات النقدية الآمنة في المستعرضات:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **الإعدادات** للانتقال إلى قسم **الإعدادات**.
3. في الجزء الأيمن من النافذة، حدد القسم **الحماية**.
4. في الجزء الأيسر من قسم **الحماية**، حدد قسم **مكافحة فيروسات الويب**.
5. في نافذة **إعدادات مكافحة فيروسات الويب** التي تفتح، انقر فوق الرابط **إعدادات متقدمة** لفتح نافذة **الإعدادات المتقدمة لمكافحة فيروسات الويب**.
6. من قسم **امتدادات مستعرض الويب**، حدد خانة الاختيار **تفعيل مكونات التطبيق الإضافية في كل مستعرضات الويب**.

حول الحماية ضد لقطات الشاشة

لحماية بياناتك عند تصفح مواقع ويب محمية، يمنع Kaspersky Total Security برامج التجسس من أخذ لقطات شاشة غير مصرح بها. يتم تمكين الحماية ضد لقطات الشاشة بشكل افتراضي. إذا تم تعطيل الحماية يدويًا، فيمكنك تمكينها في نافذة إعدادات التطبيق (انظر القسم "تمكين الحماية ضد لقطات الشاشة" على صفحة 54).

يستخدم Kaspersky Total Security تقنية hypervisor لتوفير حماية ضد لقطات الشاشة. على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Microsoft Windows 8 x64، تنطوي الحماية ضد لقطات الشاشة والتي يتم توفيرها بواسطة Kaspersky Total Security hypervisor على القيود التالي:

- لا تتوفر هذه الميزة عند تشغيل تقنية hypervisor الخاصة بطرف خارجي، مثل VMware® virtualization hypervisor. بعد غلق hypervisor الخاص بالطرف الخارجي للوقاية من لقطات الشاشة، تصبح اللقطات متاحة مرة أخرى.
- ولا تتوفر هذه الميزة إذا كانت وحدة المعالجة المركزية الخاصة بالكمبيوتر لا تدعم تقنية الأجهزة الظاهرية. لمعرفة المزيد من التفاصيل حول ما إذا كانت وحدة المعالجة المركزية الخاصة بك تدعم تقنية الأجهزة الظاهرية، يُرجى مراجعة المستندات المشحونة مع الكمبيوتر أو الاطلاع على موقع الويب الخاص بمُصَنِّع وحدة المعالجة المركزية.
- لا تتوفر هذه المزية إذا كان hypervisor الخاص بالطرف الخارجي (مثل VMware hypervisor) يعمل عند بدء المستعرض المحمي.

تمكين الحماية ضد لقطات الشاشة

لتمكين الحماية ضد لقطات الشاشة:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الإعدادات**. انتقل إلى قسم **الإعدادات**.
3. في الجزء الأيمن من النافذة، حدد القسم **الحماية**.
4. في الجزء الأيسر من القسم **الحماية** حدد القسم الفرعي **الخدمات النقدية الآمنة** وتأكد من تشغيل مفتاح الخدمات النقدية الآمنة.

   سيتم فتح نافذة **إعدادات الخدمات النقدية الآمنة**.
5. في القسم **إضافي**، حدد خانة الاختيار **منع التقاط صور الشاشة في المستعرض المحمي**.

حول حماية بيانات الحافظة

يمنع Kaspersky Total Security الوصول غير المرخص للتطبيقات إلى الحافظة عند إجراء مدفوعات عبر الإنترنت، ومن ثم يمنع سرقة البيانات بواسطة المجرمين. يتم تنشيط المنع فقط عند محاولة تطبيق غير موثوق به الحصول على وصول غير مرخص إلى الحافظة. إذا قمت بنسخ البيانات يدويًا من نافذة تطبيق إلى نافذة تطبيق آخر (على سبيل المثال، من نافذة المفكرة إلى نافذة المستعرض)، فيتم السماح بالوصول إلى الحافظة.

التحقق من أمان موقع الويب

يسمح Kaspersky Total Security بفحص سلامة موقع الويب قبل النقر فوق رابط لفتحه، ويتم فحص مواقع الويب باستخدام *مستشار Kaspersky لعناوين مواقع الويب*، المدمج في المكون "مكافحة فيروسات الويب".

لا يتوفر مستشار Kaspersky لعناوين موقع الويب في Microsoft Internet Explorer 10 و11 بنمط واجهة المستخدم الحديثة.

يتم تكامل مستشار Kaspersky لعناوين مواقع الويب في مستعرضات Microsoft Internet Explorer و Google Chrome و Mozilla Firefox، ويقوم بفحص الروابط الموجودة على صفحات الويب المفتوحة في المستعرض. يعرض Kaspersky Total Security أحد الرموز التالية بجوار كل ارتباط:

- – إذا كانت صفحة الويب المرتبطة آمنة وفقًا لـ Kaspersky Lab
- – إذا لم توجد معلومات حول حالة سلامة صفحة الويب المرتبطة
- – إذا كانت صفحة الويب المرتبطة خطرة وفقًا لـ Kaspersky Lab

لعرض نافذة منبثقة تتضمن الكثير من التفاصيل حول الرابط، حرك مؤشر الماوس إلى الرمز المعني.

بشكل افتراضي، يقوم Kaspersky Total Security بفحص الارتباطات الموجودة في نتائج البحث فقط. يمكنك تمكين فحص الارتباط على كل موقع ويب.

لتمكين التحقق من الروابط على مواقع الويب:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **الإعدادات** لفتح نافذة **الإعدادات**.

3. في القسم **الحماية**، حدد القسم الفرعي **مكافحة فيروسات الويب**.

   تعرض النافذة إعدادات مكافحة فيروسات الويب.

4. في الجزء السفلي من النافذة، انقر فوق الرابط **إعدادات متقدمة**. يتم فتح نافذة الإعدادات المتقدمة لمكافحة فيروسات الويب.

5. في القسم **مستشار Kaspersky لعناوين مواقع الويب**، حدد خانة الاختيار **التحقق من عناوين مواقع الويب**.

6. إذا كنت تريد أن يقوم المكون "مكافحة فيروسات الويب" بفحص محتوى جميع مواقع الويب، فحدد **في جميع مواقع الويب باستثناء المحددة**.

   إذا لزم الأمر، فحدد صفحات الويب التي تثق بها من خلال النقر فوق الرابط **تكوين الاستثناءات**. لا يفحص المكون "مكافحة فيروسات الويب" محتوى صفحات الويب المحدد والاتصالات المشفرة مع مواقع الويب المحددة.

7. إذا كنت تريد أن يتحقق المكون "مكافحة فيروسات الويب" من محتوى صفحات ويب معينة فقط:

   a. حدد **في جميع مواقع الويب المحددة فقط**.

   b. انقر فوق الرابط **تكوين مواقع الويب التي تم التحقق منها**.

   c. في النافذة **تكوين مواقع الويب التي تم التحقق منها** التي يتم فتحها، انقر فوق الزر **إضافة**.

   d. في النافذة **إضافة عنوان موقع ويب** التي يتم فتحها، أدخل عنوان URL لصفحة الويب التي تريد التحقق من محتواها.

   e. حدد حالة التحقق من صفحة الويب (إذا كانت الحالة *فعالاً* ، فيتحقق المكون "مكافحة فيروسات الويب" من محتوى صفحة الويب).

   f. انقر فوق الزر **إضافة**.

   تظهر صفحة الويب المحددة في القائمة الموجودة في النافذة **مواقع الويب التي تم التحقق منها**. يتحقق المكون "مكافحة فيروسات الويب" من عناوين مواقع الويب الموجودة على صفحة الويب هذه.

8. إذا كنت تريد تحرير الإعدادات المتقدمة للتحقق من عناوين مواقع الويب، من نافذة **الإعدادات المتقدمة لمكافحة فيروسات الويب**، في **مستشار Kaspersky لعناوين مواقع الويب**، انقر فوق الرابط **تكوين مستشار Kaspersky لعناوين مواقع الويب**.

   يتم فتح النافذة **تكوين مستشار Kaspersky لعناوين مواقع الويب**.

9. إذا كنت تريد أن يخبرك المكون "مكافحة فيروسات الويب" بأمان الروابط على جميع صفحات الويب، فمن **التحقق من عناوين مواقع الويب**، حدد **كل عناوين مواقع الويب**.

10. إذا كنت تريد أن يعرض المكون "مكافحة فيروسات الويب" معلومات حول ما إذا كان الرابط ينتمي إلى فئة معينة من محتوى مواقع الويب (مثل *الألفاظ النابية والفحش*):

    a. فحدد خانة الاختيار **إظهار معلومات حول فئات محتوى مواقع الويب**.

    b. حدد خانات الاختيار بجوار فئات محتوى مواقع الويب التي ينبغي عرض معلومات حولها في تعليقات.

يتحقق المكون "مكافحة فيروسات الويب" من الروابط على صفحات الويب المحددة، ويعرض معلومات حول فئات الروابط وفقًا للإعدادات الحالية.

بدء تشغيل KASPERSKY PASSWORD MANAGER

يمكن الغرض من Kaspersky Password Manager في تعبئة حقول الإدخال تلقائيًا على مواقع الويب وفي تطبيقات Microsoft Windows. يجب تثبيت Kaspersky Password Manager بشكل مستقل عن Kaspersky Total Security. بعد تثبيت Kaspersky Password Manager، يمكنك بدء تشغيله من القائمة **ابدأ** أو من نافذة Kaspersky Total Security.

لبدء تشغيل Kaspersky Password Manager الذي تم تثبيته بالفعل:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الزر **مدير كلمات المرور**.

يتم فتح نافذة Kaspersky Password Manager.

لبدء تشغيل Kaspersky Password Manager الذي تم تثبيته بعد:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الزر **مدير كلمات المرور**.

   يتم فتح نافذة **مدير كلمات مرور**.

3. انقر فوق الزر **تنزيل الإصدار الجديد** في نافذة **Password Manager**.

   سيتم أخذك إلى موقع ويب Kaspersky Lab حيث يمكنك تنزيل حزمة تثبيت Kaspersky Password Manager. إذا كان لديك إصدار سابق لـ Kaspersky Password Manager مثبت على الكمبيوتر، فسوف يطالبك Kaspersky Total Security بترقية إصدار Kaspersky Password Manager.

راجع دليل مستخدم *Kaspersky Password Manager* للحصول على تعليمات حول استخدام Kaspersky Password Manager.

إزالة تتبعات النشاط على الكمبيوتر والإنترنت

يتم تسجيل إجراءات المستخدم على الكمبيوتر في نظام التشغيل. يتم حفظ المعلومات التالية:

- تفاصيل بحث الاستعلامات التي يقوم المستخدمين ومواقع الويب بإدخالها
- معلومات حول التطبيقات التي تم تشغيلها بالإضافة إلى الملفات المفتوحة والمحفوظة
- إدخالات سجلات أحداث Microsoft Windows
- معلومات أخرى حول نشاط المستخدم

قد يتمكن المتطفلون والأشخاص غير المرخصين من الوصول إلى المعلومات الشخصية المضمنة في البيانات حول إجراءات المستخدم الماضية.

يشتمل Kaspersky Total Security على "معالج منظف الخصوصية" الذي ينظف آثار نشاط المستخدم في نظام التشغيل.

لتشغيل معالج منظف الخصوصية:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.
3. في الجزء الأيمن من نافذة **الأدوات**، انقر فوق الرابط **منظف الخصوصية** لتشغيل معالج منظف الخصوصية.

يتكون "المعالج" من سلسلة من الصفحات (الخطوات) التي يمكنك التنقل بينها بالنقر فوق الزرين **رجوع** و**التالي**. لإغلاق "المعالج" بعد انتهائه، انقر فوق الزر **إنهاء**. لإيقاف المعالج في أي مرحلة، انقر الزر **إلغاء**.

دعنا نقوم بمراجعة خطوات المعالج بقدر أكبر من التفصيل.

الخطوة 1. بدء تشغيل المعالج

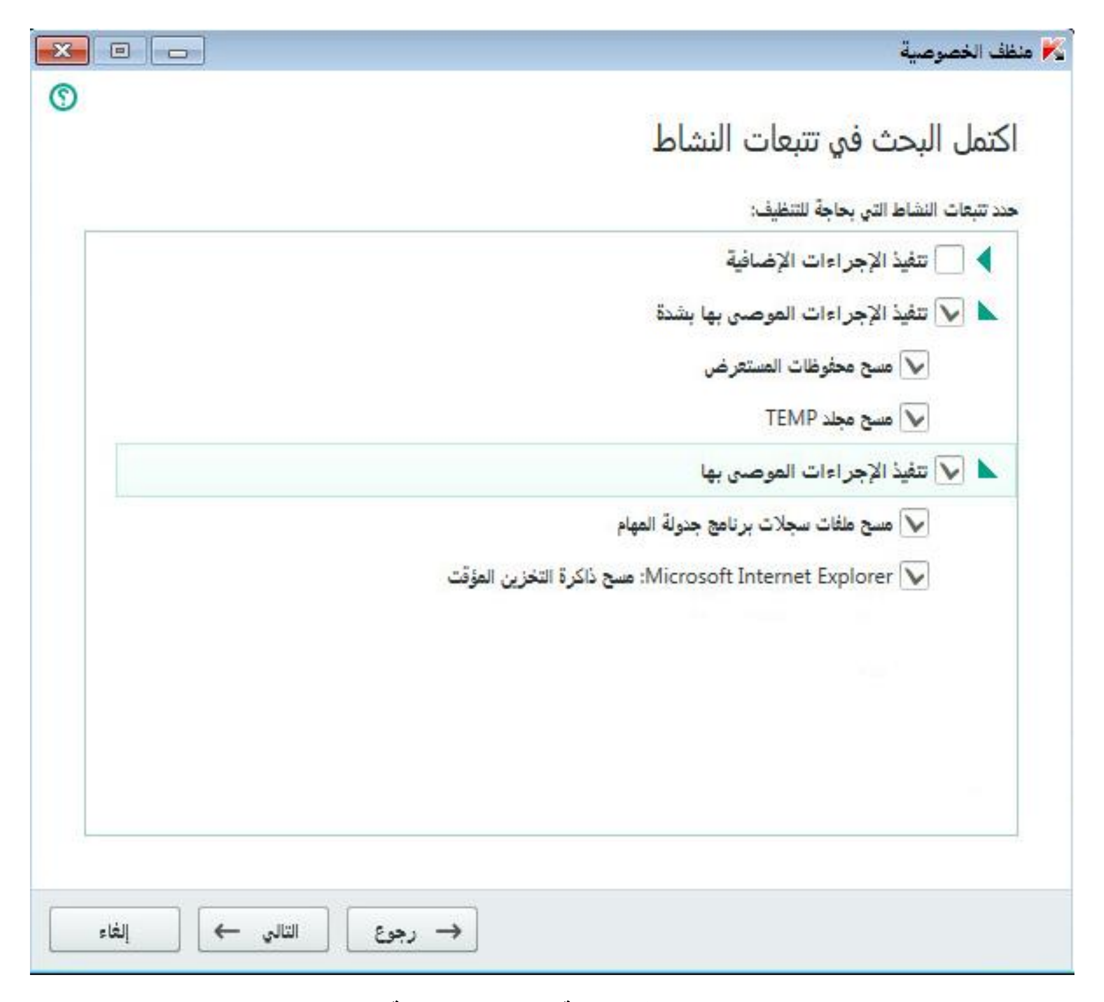
تأكد من تحديد خانة الاختيار **البحث عن تتبعات نشاط المستخدم**. انقر الزر **التالي** لبدء المعالج.

الخطوة 2. البحث في تتبعات النشاط

يقوم هذا المعالج بالبحث عن تتبعات النشاط على جهاز الكمبيوتر. قد يستغرق البحث بعض الوقت. وبمجرد أن ينتهي البحث، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

الخطوة 3. تحديد إجراءات منظف الخصوصية

عند اكتمال البحث، يخبرك "المعالج" حول تتبعات النشاط المكتشفة ويطلب منك تحديد الإجراءات المطلوب القيام بها للتخلص من التتبعات المكتشفة للنشاط (انظر الشكل التالي).



الشكل 4. تتبعات النشاط المكتشفة والتوصيات الخاصة بالقضاء عليها

لعرض الإجراءات داخل أي مجموعة، انقر الرمز ◀ الموجود على يمين اسم المجموعة.

لجعل المعالج يقوم بتنفيذ إجراء معين، حدد خانة الاختيار الموجودة على يمين الإجراء المعني. وافتراضيًا، ينفذ المعالج جميع الإجراءات المستحسنة والمستحسنة بشدة. إذا كنت لا ترغب في تنفيذ إجراء معين، فقم بإلغاء تحديد خانة الاختيار المجاورة له.

لا يوصى بإلغاء تحديد خانات الاختيار المحددة بشكل افتراضي. قد يؤدي هذا الأمر إلى تعريض أمان الكمبيوتر الخاص بك للخطر.

بعد تحديد مجموعة الإجراءات التي سيقوم المعالج بتنفيذها، انقر فوق زر **التالي**.

الخطوة 4. تنظيف تتبعات النشاط:

سينفذ المعالج الإجراءات المحددة أثناء الخطوة السابقة. وقد يستغرق التخلص من تتبعات النشاط بعض الوقت. لتنظيف تتبعات نشاط معين، قد يكون من الضروري إعادة تشغيل الكمبيوتر؛ وإذا كان الأمر كذلك، فسيخبرك المعالج.

وعندما ينتهي التنظيف، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

الخطوة 5. اكتمال المعالج

انقر الزر **إنهاء** لإغلاق المعالج.

التحكم في أنشطة المستخدمين الموجودة على الكمبيوتر والإنترنت

يقدم هذا القسم معلومات حول كيفية التحكم في إجراءات المستخدمين على الكمبيوتر والإنترنت باستخدام Kaspersky Total Security.

في هذا القسم

استخدام الرقابة الأسرية

تتيح لك *الرقابة الأسرية* مراقبة الإجراءات التي تم إجراؤها بواسطة المستخدمين على كمبيوتر محلي أو عبر الإنترنت. يمكنك استخدام الرقابة الأسرية لتقييد الوصول إلى موارد الإنترنت والتطبيقات، إلى جانب إمكانية عرض تقارير حول أنشطة المستخدمين.

يتزايد عدد الأطفال والمراهقين الذين يمكنهم الوصول إلى أجهزة كمبيوتر وموارد الويب. يمثل استخدام أجهزة الكمبيوتر والإنترنت عددًا من التحديات والتهديدات للأطفال:

- إهدار الوقت و / أو النقود عند زيارة غرف الدردشة، وموارد الألعاب، والمتاجر على الإنترنت، والمزادات
- الوصول إلى مواقع ويب تستهدف البالغين، مثل تلك التي تعرض محتوى يدور حول الإباحية، والتطرف، والأسلحة، وتعاطي المخدرات، والعنف الصريح
- تنزيل ملفات مصابة ببرمجيات خبيثة؛
- الإضرار بالصحة نتيجة الاستخدام الزائد للكمبيوتر
- الاتصال بأشخاص غير مألوفين من الذين يتظاهرون بالصداقة للحصول على معلومات شخصية من المستخدمين الصغار، مثل الاسم الحقيقي، والعنوان الفعلي، والوقت الذي لا يكون فيه أحد موجودًا في المنزل

يمكنك مكون الرقابة الأسرية من تقليل المخاطر التي يشكلها الكمبيوتر والإنترنت. للقيام بذلك، تتوفر الوظائف التالية:

- تحديد وقت استخدام الكمبيوتر والإنترنت.
- إنشاء قوائم بالألعاب والتطبيقات المسموح بها والممنوعة، إلى جانب التقييد المؤقت لاستخدام التطبيقات المسموح بها.
- إنشاء قوائم بمواقع الويب المسموح بها والممنوعة، مع تحديد فئات مواقع الويب التي تحتوي على محتوى غير مناسب.

- تمكين وضع البحث الآمن على محركات البحث (عدم عرض ارتباطات مواقع الويب التي بها محتوى مريب ضمن نتائج البحث).
- تقييد عمليات تحميل الملفات من الإنترنت.
- إنشاء قوائم بجهات الاتصال المسموح بها أو الممنوعة لعملاء المراسلة الفورية (IM) وشبكات التواصل الاجتماعي.
- عرض سجلات الرسائل من برامج المراسلة الفورية (IM) وشبكات التواصل الاجتماعي.
- منع إرسال بيانات شخصية معينة.
- البحث عن كلمات رئيسية معينة في سجلات الرسائل.

يمكنك تكوين مزايا "الرقابة الأسرية" لكل حساب مستخدم على الكمبيوتر على حدة. يمكنك أيضًا عرض تقارير "الرقابة الأسرية" حول أنشطة المستخدمين الخاضعين للرقابة.

الانتقال إلى إعدادات الرقابة الأسرية

للانتقال إلى إعدادات الرقابة الأسرية:

1. افتح نافذة التطبيق الرئيسية.
2. في نافذة التطبيق الرئيسية، انقر فوق الزر **الرقابة الأسرية**.
3. عند فتح نافذة **الرقابة الأسرية** لأول مرة، يُطالبك التطبيق بتعيين كلمة مرور لحماية إعدادات الرقابة الأسرية. حدد أحد الخيارات التالية:
   - إذا كنت تريد وصولاً محميًا بكلمة مرور إلى إعدادات الرقابة الأسرية، فاملأ حقول **كلمة المرور** و**تأكيد** ثم انقر فوق الزر **متابعة**.
   - إذا كنت تريد وصولاً محميًا بكلمة مرور إلى إعدادات الرقابة الأسرية، فانقر فوق الرابط **تخطي** للمتابعة إلى إعدادات الرقابة الأسرية.

   يتم فتح النافذة **الرقابة الأسرية**.
4. حدد حساب مستخدم وانقر فوق الرابط **تكوين القيود** لفتح نافذة إعدادات الرقابة الأسرية.

التحكم في استخدام الكمبيوتر

تتيح لك "المراقبة الأسرية" تحديد مقدار الوقت الذي يقضيه المستخدم على الكمبيوتر. يمكنك تحديد فترة زمنية ينبغي أن تقوم خلالها "الرقابة الأسرية" بمنع الوصول إلى الكمبيوتر (وقت النوم)، إلى جانب إمكانية تحديد الحد الزمني اليومي لاستخدام الكمبيوتر. يمكنك تحديد حدود زمنية مختلفة لأيام الأسبوع وعطلات نهاية الأسبوع.

لتكوين الحدود الزمنية لاستخدام الكمبيوتر:

1. انتقل إلى نافذة إعدادات الرقابة الأسرية (انظر القسم "الانتقال إلى إعدادات الرقابة الأسرية" على صفحة 60).
2. في نافذة إعدادات الرقابة الأسرية، حدد قسم **الكمبيوتر**.
3. لتحديد فاصل زمني ستقوم خلاله الرقابة الأسرية بمنع الوصول إلى الكمبيوتر، في الأقسام **أيام الأسبوع** و**عطلات نهاية الأسبوع**، حدد خانة الاختيار **منع الوصول من**.
4. في القائمة المنسدلة المجاورة لخانة الاختيار **منع الوصول من**، حدد وقت بدء المنع.

5. في القائمة المنسدلة **إلى** حدد وقت انتهاء المنع.

يمكنك إعداد جدول زمني لاستخدام الكمبيوتر باستخدام جدول. لعرض الجدول، انقر فوق الزر .

ستمنع "الرقابة الأسرية" وصول المستخدم إلى الكمبيوتر خلال الفترة الزمنية المحددة.

6. لتعيين حد زمني لإجمالي استخدام الكمبيوتر على مر اليوم، في الأقسام **أيام الأسبوع** و**عطلات نهاية الأسبوع** حدد خانة الاختيار **السماح بالوصول لمدة لا تزيد عن** ومن القائمة المنسدلة المجاورة لخانة الاختيار حدد فاصلاً زمنيًا.

تمنع الرقابة الأسرية وصول المستخدم إلى الكمبيوتر عند تجاوز إجمالي استخدام الكمبيوتر المقدار الزمني المحدد.

7. لإعداد فترات راحة في جلسات استخدام المستخدم للكمبيوتر، في قسم **فواصل زمنية**، حدد خانة الاختيار **أخذ راحة كل** ثم من القوائم المنسدلة المجاورة لخانة الاختيار حدد قيمًا لتكرار فترات الراحة (على سبيل المثال، كل ساعة) وطولها (على سبيل المثال، 10 دقائق).

8. في النافذة **الرقابة الأسرية**، قم بتفعيل مفتاح **الرقابة الأسرية** الموجود بجوار حساب المستخدم.

ستمنع "الرقابة الأسرية" وصول المستخدم إلى الكمبيوتر وفقًا للإعدادات الجديدة.

التحكم في استخدام الإنترنت

باستخدام "الرقابة الأسرية"، يمكنك تحديد الوقت المنقضي على الإنترنت ومنع المستخدمين من الوصول إلى فئات معينة من مواقع الويب أو مواقع ويب معينة. يمكنك أيضًا منع المستخدم من تنزيل أنواع معينة من الملفات (مثل الأرشيفات أو مقاطع الفيديو) من الإنترنت.

لتعيين الحد الزمني لاستخدام الإنترنت:

1. انتقل إلى نافذة إعدادات الرقابة الأسرية (انظر القسم "الانتقال إلى إعدادات الرقابة الأسرية" على صفحة 60).
2. في نافذة إعدادات الرقابة الأسرية، حدد قسم **الإنترنت**.
3. إذا كنت تريد تحديد إجمالي وقت استخدام الإنترنت في أيام الأسبوع، ففي قسم **تقييد الوصول إلى الإنترنت**، حدد خانة الاختيار **تقييد الوصول في أيام الأسبوع إلى <ساعات:دقائق> ساعة يوميًا** ثم حدد قيمة للحد الزمني من القائمة المنسدلة المجاورة لخانة الاختيار.
4. إذا كنت تريد تحديد إجمالي وقت استخدام الإنترنت في عطلات نهاية الأسبوع، فحدد خانة الاختيار **تقييد الوصول في عطلات نهاية الأسبوع إلى <ساعات:دقائق> ساعة يوميًا**، ثم حدد قيمة للحد الزمني من القائمة المنسدلة المجاورة لخانة الاختيار.
5. في النافذة **الرقابة الأسرية**، قم بتفعيل مفتاح **الرقابة الأسرية** الموجود بجوار حساب المستخدم.

ستحدد "الرقابة الأسرية" إجمالي الوقت الذي يقضيه المستخدم على الإنترنت وفقًا للقيم التي قمت بتحديدها.

لتقييد الزيارات إلى مواقع ويب معينة:

1. انتقل إلى نافذة إعدادات الرقابة الأسرية (انظر القسم "الانتقال إلى إعدادات الرقابة الأسرية" على صفحة 60).
2. في نافذة إعدادات الرقابة الأسرية، حدد قسم **الإنترنت**.
3. لتجنب عرض محتوى بالغين في نتائج البحث، من القسم **التحكم في تصفح الويب**، حدد خانة الاختيار **تمكين البحث الآمن**.

عند البحث عن معلومات على مواقع ويب مثل Google™ وYouTube™ (فقط للمستخدمين الذين لم يقوموا بتسجيل الدخول إلى موقع ويب youtube.com من حسابهم) وBing® وYahoo!™ وMail.ru وVKontakte وYandex، لا يتم عرض محتوى بالغين في نتائج البحث.

4. لمنع الوصول إلى مواقع ويب من فئات معينة:

a. في القسم **التحكم في تصفح الويب**، حدد خانة الاختيار **منع الوصول إلى مواقع الويب التالية**.

b. حدد **مواقع ويب للبالغين**/ وانقر فوق الرابط **تحديد فئات من مواقع ويب** لفتح النافذة **منع الوصول إلى فئات مواقع الويب**.

c. حدد خانات الاختيار المجاورة لفئات مواقع الويب التي تريد منعها.

ستمنع "الرقابة الأسرية" جميع محاولات المستخدم لفتح موقع الويب إذا كان محتواه مصنفًا بأنه ينتمي إلى أي من الفئات الممنوعة.

5. لمنع الوصول إلى مواقع ويب معينة:

a. في القسم **التحكم في تصفح الويب**، حدد خانة الاختيار **منع الوصول إلى مواقع الويب التالية**.

b. حدد **يُسمح في القائمة بكل مواقع ويب عدا الاستثناءات**، وانقر فوق الرابط **إضافة استثناءات** لفتح النافذة **الاستثناءات**.

c. في الجزء السفلي من النافذة، انقر فوق زر **إضافة**.

يتم فتح النافذة **إضافة موقع ويب جديد**.

d. أدخل عنوان موقع الويب الذي تريد منع زيارته من خلال ملء الحقل **عنوان الويب**.

e. في قسم **النطاق**، حدد نطاق ما تريد منعه: موقع الويب بأكمله أو صفحة ويب محددة فقط.

f. إذا كنت تريد منع موقع الويب المحدد، من القسم **الإجراء**، حدد **منع**.

g. انقر فوق الزر **إضافة**.

يظهر موقع الويب المحدد في القائمة الموجودة في النافذة **الاستثناءات**.

6. في النافذة **الرقابة الأسرية**، قم بتفعيل مفتاح **الرقابة الأسرية** الموجود بجوار حساب المستخدم.

ستمنع "الرقابة الأسرية" جميع محاولات المستخدم لفتح أي موقع ويب مدرج وفقًا للإعدادات الحالية.

لمنع تنزيل أنواع معينة من الملفات من الإنترنت:

1. انتقل إلى نافذة إعدادات الرقابة الأسرية (انظر القسم "الانتقال إلى إعدادات الرقابة الأسرية" على صفحة 60).

2. في نافذة إعدادات الرقابة الأسرية، حدد قسم **الإنترنت**.

3. في القسم **وضع حدود لتنزيل الملفات**، حدد خانات الاختيار المجاورة لأنواع الملفات التي تريد منع تنزيلها.

4. في النافذة **الرقابة الأسرية**، قم بتفعيل مفتاح **الرقابة الأسرية** الموجود بجوار حساب المستخدم.

ستمنع "الرقابة الأسرية" تنزيل الأنواع المحدد من الملفات من الإنترنت.

التحكم في بدء تشغيل الألعاب والتطبيقات

باستخدام "الرقابة الأسرية"، يمكنك السماح للمستخدم ببدء الألعاب أو منعه من بدئها حسب تصنيفات الألعاب العمرية. يمكنك منع المستخدم من بدء تطبيقات معينة (مثل الألعاب أو عملاء المراسلة الفورية) أو تقييد الوقت المسموح به لاستخدام التطبيقات.

لمنع الألعاب المزودة بمحتوى غير مناسب لفئة عمرية:

1. انتقل إلى نافذة إعدادات الرقابة الأسرية (انظر القسم "الانتقال إلى إعدادات الرقابة الأسرية" على صفحة 60).
2. في نافذة إعدادات الرقابة الأسرية، حدد القسم **التطبيقات**.
3. في القسم **منع الألعاب حسب المحتوى**، يمكنك منع بدء تشغيل الألعاب غير الملائمة للمستخدم المحدد بناءً على العمر / و أو المحتوى:
   a. إذا كنت تريد منع جميع الألعاب التي تحتوي على محتوى غير مناسب لعمر المستخدم، فحدد خانة الاختيار **منع الألعاب حسب التصنيف العمري** وحدد خيار التقييد العمري من القائمة المنسدلة المجاورة لخانة الاختيار.
   b. إذا كنت تريد منع الألعاب ذات المحتوى من فئة معينة:
      a. حدد خانة الاختيار **منع الألعاب من الفئات البالغة**.
      b. انقر فوق الرابط **تحديد فئات الألعاب** لفتح النافذة **منع الألعاب حسب الفئات**.
      c. حدد خانات الاختيار المجاورة لفئات المحتوى المناظرة للألعاب التي تريد منعها.
4. في النافذة **الرقابة الأسرية**، قم بتفعيل مفتاح **الرقابة الأسرية** الموجود بجوار حساب المستخدم.

لتقييد بدء تشغيل تطبيق معين:

1. انتقل إلى نافذة إعدادات الرقابة الأسرية (انظر القسم "الانتقال إلى إعدادات الرقابة الأسرية" على صفحة 60).
2. في نافذة إعدادات الرقابة الأسرية، حدد القسم **التطبيقات**.
3. في الجزء السفلي من النافذة، انقر فوق الرابط **إضافة تطبيق إلى القائمة** لفتح مربع الحوار **فتح** وحدد ملف التطبيق القابل للتنفيذ.

   يظهر التطبيق المحدد في القائمة في القسم **منع التطبيقات المحددة**. يضيف Kaspersky Total Security التطبيق تلقائيًا إلى فئة محددة، مثل *"ألعاب"*.
4. إذا كنت تريد منع أحد التطبيقات، فحدد خانة الاختيار المجاورة لاسم التطبيق في القائمة. يمكنك أيضًا منع جميع التطبيقات التي تنتمي إلى فئة محددة بتحديد خانة الاختيار المجاورة لاسم الفئة في القائمة (فيمكنك منع الفئة *ألعاب* على سبيل المثال).
5. إذا كنت تريد تقييد مدة استخدام تطبيق، فحدد تطبيقًا أو فئة تطبيقات من القائمة وانقر فوق الرابط **تكوين القواعد** لفتح نافذة **قيود استخدام التطبيق**.
6. إذا كنت ترغب في تعيين حد زمني لاستخدام التطبيق أيام الأسبوع وأيام عطلات نهاية الأسبوع، في الأقسام **أيام الأسبوع** و**عطلات نهاية الأسبوع**، حدد خانة الاختيار **السماح بالوصول لمدة لا تزيد عن** وفي القائمة المنسدلة حدد عدد الساعات المسموح للمستخدم فيها استخدام التطبيق يوميًا. يمكنك أيضًا تحديد الوقت الذي يُسمح فيه للمستخدم باستخدام التطبيق / يُمنع من استخدامه من خلال استخدام جدول لذلك. لعرض الجدول، انقر فوق الزر .
7. إذا كنت تريد تعيين توقفات مؤقتة في استخدام التطبيق، في القسم **فواصل زمنية**، فحدد خانة الاختيار **أخذ راحة كل** ومن القوائم المنسدلة حدد القيم لتكرار الفاصل ومدته.
8. انقر فوق الزر **حفظ**.

9. في النافذة **الرقابة الأسرية**، قم بتفعيل مفتاح **الرقابة الأسرية** الموجود بجوار حساب المستخدم.

ستُطبق "الرقابة الأسرية" القيود المحددة عند وصول المستخدم إلى التطبيق.

التحكم في المراسلة على شبكات التواصل الاجتماعي

باستخدام "الرقابة الأسرية"، يمكنك عرض مراسلات المستخدم عبر شبكات التواصل الاجتماعي وبرامج المراسلة الفورية (IM)، إلى جانب إمكانية منع المراسلات مع جهات اتصال معينة.

تكوين مراقبة مراسلات المستخدم:

1. انتقل إلى نافذة إعدادات الرقابة الأسرية (انظر القسم "الانتقال إلى إعدادات الرقابة الأسرية" على صفحة 60).
2. في نافذة إعدادات الرقابة الأسرية، حدد قسم **التواصل**.
3. لعرض سجلات المراسلات ومنع جهات اتصال معينة إذا لزم الأمر:
   a. حدد **منع المراسلة مع جميع جهات الاتصال باستثناء جهات الاتصال المسموح بها**.
   b. انقر فوق الرابط **جهات الاتصال** لفتح النافذة **جهات الاتصال**.
   c. اعرض جهات الاتصال التي قام المستخدم بمراسلتهم. يمكنك عرض جهات اتصال معينة في النافذة باستخدام إحدى الطرق التالية:
      - لعرض سجلات مراسلة المستخدم عبر شبكة اجتماعية معينة أو عميل مراسلة فورية، حدد العنصر المطلوب من القائمة المنسدلة في الجزء الأيمن من النافذة.
      - لعرض جهات اتصال تراسل معها المستخدم بشكل أكثر فعّالية، من القائمة المنسدلة في الجانب الأيسر من النافذة، حدد **حسب عدد الرسائل**.
      - لعرض جهات اتصال تراسل معها المستخدم في يوم محدد، من القائمة المنسدلة في الجانب الأيسر من النافذة، حدد **حسب تاريخ المراسلة**.
   d. لعرض مراسلات المستخدم مع جهة اتصال معينة، انقر فوق جهة الاتصال من القائمة.

      يتم فتح النافذة **سجل المراسلة**.
   e. إذا كنت تريد منع مراسلات المستخدم مع جهة الاتصال المحددة، فانقر فوق الزر **منع**.
4. في النافذة **الرقابة الأسرية**، قم بتفعيل مفتاح **الرقابة الأسرية** الموجود بجوار حساب المستخدم.

ستمنع "الرقابة الأسرية" تبادل الرسائل بين المستخدم وجهة الاتصال المحدد.

مراقبة محتويات الرسالة

باستخدام "الرقابة الأسرية"، يمكنك مراقبة محاولات المستخدم لإدراج بيانات خاصة (مثل الأسماء، وأرقام الهواتف، وأرقام البطاقات البنكية) وكلمات مفتاحية معينة (مثل الكلمات البذيئة) في الرسائل، كما يمكنك منع ذلك أيضًا.

تكوين التحكم في نقل البيانات الخاصة:

1. انتقل إلى نافذة إعدادات الرقابة الأسرية (انظر القسم "الانتقال إلى إعدادات الرقابة الأسرية" على صفحة 60).
2. في نافذة إعدادات الرقابة الأسرية، حدد قسم **التحكم في المحتوى**.

3. في القسم **مراقبة نقل البيانات الخاصة**، حدد خانة الاختيار **منع نقل البيانات الخاصة إلى جهات خارجية**.
4. انقر فوق الرابط **تحرير قائمة البيانات الخاصة** لفتح النافذة **قائمة البيانات الخاصة**.
5. في الجزء السفلي من النافذة، انقر فوق زر **إضافة**.

   يتم فتح نافذة لإضافة البيانات الخاصة.
6. حدد نوع البيانات الخاصة (على سبيل المثال، "رقم الهاتف") عن طريق النقر فوق الرابط المناظر أو إدخال وصف في حقل **اسم المجال**.
7. حدد البيانات الخاصة (مثل اسمك الأخير أو رقم هاتفك) في حقل **القيمة**.
8. انقر فوق الزر **إضافة**.

   ستم إدراج البيانات الخاصة في النافذة **قائمة البيانات الخاصة**.
9. في النافذة **الرقابة الأسرية**، قم بتفعيل مفتاح **الرقابة الأسرية** الموجود بجوار حساب المستخدم.

ستراقب "الرقابة الأسرية" محاولات المستخدم لاستخدام البيانات الخاصة المحدد في المراسلات عبر برامج المراسلة الفورية (IM) وعلى مواقع الويب، كما أنها ستمنع ذلك.

لتكوين التحكم في الكلمات المفتاحية للرسائل:

1. انتقل إلى نافذة إعدادات الرقابة الأسرية (انظر القسم "الانتقال إلى إعدادات الرقابة الأسرية" على صفحة 60).
2. في نافذة إعدادات الرقابة الأسرية، حدد قسم **التحكم في المحتوى**.
3. في القسم **التحكم في الكلمات المفتاحية**، حدد خانة الاختيار **تمكين التحكم في الكلمات المفتاحية**.
4. انقر فوق الرابط **تحرير قائمة الكلمات الرئيسية** لفتح النافذة **التحكم في الكلمات المفتاحية**.
5. في الجزء السفلي من النافذة، انقر فوق زر **إضافة**.

   يتم فتح نافذة لإضافة كلمة مفتاحية.
6. أدخل عبارة مفتاحية في الحقل **القيمة**، وانقر فوق الزر **إضافة**.

   تظهر العبارة المفتاحية المحددة في قائمة الكلمات المفتاحية في النافذة **التحكم في الكلمات المفتاحية**.
7. في النافذة **الرقابة الأسرية**، قم بتفعيل مفتاح **الرقابة الأسرية** الموجود بجوار حساب المستخدم.

ستمنع "الرقابة الأسرية" إرسال الرسائل التي تتضمن العبارة المفتاحية المحددة أثناء المراسلات عبر الإنترنت أو عبر برامج عملاء المراسلة الفورية.

عرض تقرير حول نشاط المستخدم

يمكنك الوصول إلى تقارير حول نشاط كل حساب مستخدم يتم التحكم فيه بواسطة الرقابة الأسرية، وذلك بإعداد تقارير منفصلة لكل فئة من الأحداث الخاضعة للتحكم.

لعرض تقرير حول نشاط حساب مستخدم خاضع للتحكم:

1. انتقل إلى نافذة إعدادات الرقابة الأسرية (انظر القسم "الانتقال إلى إعدادات الرقابة الأسرية" على صفحة 60).
2. حدد حساب مستخدم وانقر فوق الرابط **عرض التقرير** للانتقال إلى نافذة التقارير.

3. في قسم النوع المطلوب من التقييد (على سبيل المثال **الإنترنت** أو **التواصل**)، افتح التقرير حول الإجراءات الخاضعة للمراقبة بالنقر فوق الرابط **التفاصيل**.

تعرض النافذة تقريرًا حول إجراءات المستخدم الخاضعة للمراقبة.

إدارة حماية الكمبيوتر عن بُعد

يوضح هذا القسم كيفية إدارة حماية الكمبيوتر عن بُعد بواسطة Kaspersky Total Security مثبت.

في هذا القسم

حول إدارة حماية الكمبيوتر عن بُعد

إذا كان الكمبيوتر مثبت عليه Kaspersky Total Security، فيمكنك إدارة حماية هذا الكمبيوتر عن بُعد. يمكن إدارة حماية الكمبيوتر عن بُعد بواسطة مدخل My Kaspersky. لإدارة حماية الكمبيوتر عن بُعد، قم بالتسجيل على مدخل My Kaspersky وقم بتسجيل الدخول إلى حساب My Kaspersky الخاص بك وانتقل إلى قسم **الأجهزة**.

يتيح لك مدخل My Kaspersky إنجاز مهام أمان الكمبيوتر التالية:

- عرض قائمة بمشكلات أمان الكمبيوتر وإصلاحها عن بُعد
- فحص الكمبيوتر لاكتشاف الفيروسات والتهديدات الأخرى
- تحديث قواعد البيانات ووحدات التطبيق
- تكوين مكونات Kaspersky Total Security

إذا تم بدء تشغيل فحص الكمبيوتر من مدخل My Kaspersky، فيقوم Kaspersky Total Security بمعالجة الكائنات التي تم حذفها تلقائيًا بدون مشاركتك. عند اكتشاف فيروس أو تهديد آخر، يحاول Kaspersky Total Security إجراء التنظيف بدون إعادة تمهيد الكمبيوتر. إذا كان التنظيف بدون إعادة تشغيل الكمبيوتر غير محتمل، فتعرض قائمة مشكلات أمان الكمبيوتر على مدخل My Kaspersky رسالة بأن الكمبيوتر يحتاج إلى إعادة التشغيل لإجراء التنظيف.

الانتقال إلى الإدارة عن بُعد لحماية الكمبيوتر

للانتقال إلى الإدارة عن بُعد لحماية الكمبيوتر:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الزر **إدارة الأجهزة**.
3. في نافذة **إدارة الأجهزة**، انقر فوق الزر **توصيل الكمبيوتر بـ My Kaspersky**.

   يتم تحميل نموذج تسجيل الدخول إلى مدخل My Kaspersky في نافذة **إدارة الأجهزة** ما لم تقم بتسجيل الدخول بالفعل. قم بتعبئة الحقول ثم قم بالتسجيل على مدخل My Kaspersky.

   يتم فتح صفحة مدخل My Kaspersky مع قسم **الأجهزة** في نافذة المستعرض بشكل افتراضي.

الحفاظ على موارد نظام التشغيل لألعاب الكمبيوتر

عند تشغيل Kaspersky Total Security في وضع الوظائف الكاملة مع بعض التطبيقات الأخرى (ألعاب الكمبيوتر على وجه الخصوص)، قد تحدث المشكلات التالية:

- ينخفض أداء التطبيق أو أداء إحدى الألعاب نتيجة قلة موارد النظام.
- تشتت نوافذ إخطارات Kaspersky Total Security انتباه المستخدم عن اللعبة.

لتجنب تغيير إعدادات Kaspersky Total Security يدويًا كل مرة تقوم فيها بالتبديل إلى وضع الشاشة الكاملة، يمكنك استخدام "ملف بيانات الألعاب". عند تمكين "ملف بيانات الألعاب"، فإن التبديل إلى وضع الشاشة الكاملة يغير تلقائيًا إعدادات جميع مكونات Kaspersky Total Security، الأمر الذي يضمن الأداء المثالي للنظام في هذا الوضع. بعد الخروج من وضع ملء الشاشة، تعود إعدادات التطبيق إلى القيم الأولية المستخدمة قبل تفعيل وضع ملء الشاشة.

لتمكين "ملف بيانات الألعاب":

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **الإعدادات** للانتقال إلى قسم **الإعدادات**.
3. في الجزء الأيمن من النافذة، حدد القسم **الأداء**.

   تعرض النافذة إعدادات أداء Kaspersky Total Security.
4. في القسم **ملف بيانات الألعاب**، حدد خانة الاختيار **استخدام ملف تعريف الألعاب**.

التعامل مع التطبيقات غير المعروفة

يساعد Kaspersky Total Security على تقليل المخاطر المرتبطة باستخدام التطبيقات غير المعروفة إلى أدنى الحدود (مثل خطر الإصابة بالفيروسات والبرامج الخبيثة الأخرى والتغييرات غير المرغوب فيها التي تحدث لإعدادات نظام التشغيل).

يتضمن Kaspersky Total Security مكونات وأدوات تتيح التحقق من سمعة التطبيق والتحكم في أنشطته على الكمبيوتر.

في هذا القسم

فحص سمعة التطبيق

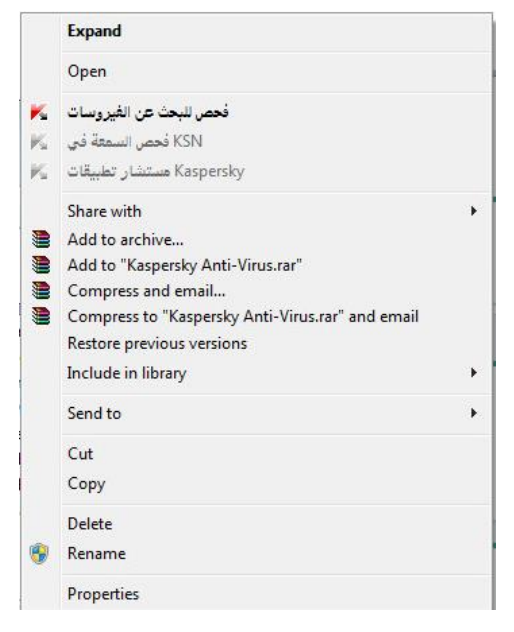
يتيح لك Kaspersky Total Security التحقق من سمعة التطبيقات من المستخدمين من جميع أرجاء العالم. تتضمن سمعة التطبيق المعايير التالية:

- اسم البائع
- معلومات حول التوقيع الرقمي (إذا تم توقيع التطبيق رقميًا)
- معلومات حول المجموعة التي تم تعيين التطبيق لها بواسطة التحكم في التطبيق أو بواسطة معظم مستخدمي شبكة أمان Kaspersky
- عدد مستخدمي Kaspersky Security Network الذين يستخدمون التطبيق (يكون متاحًا إذا كان التطبيق مُضمَّنًا في المجموعة "موثوق" في قاعدة بيانات شبكة أمان Kaspersky)؛
- الوقت الذي أصبح فيه التطبيق معروفًا في شبكة أمان Kaspersky
- أكثر الدول التي ينتشر بها التطبيق

يتوفر فحص سمعة التطبيق إذا وافقت على المشاركة في شبكة أمان Kaspersky.

لمعرفة سمعة أحد التطبيقات:

افتح الملف القابل للتنفيذ الخاص بالتطبيق، وحدد **فحص السمعة في KSN** (انظر الشكل التالي).



الشكل *5*. القائمة السياقية للكائن

سيتم فتح نافذة تتضمن معلومات حول سمعة التطبيق في KSN.

انظر أيضًا:

التحكم في أنشطة التطبيقات الموجودة على الكمبيوتر والشبكة

يمنع التحكم في التطبيق التطبيقات من تنفيذ الإجراءات التي قد تكون خطرة على نظام التشغيل، ويتحكم في الوصول إلى موارد نظام التشغيل وبياناتك الشخصية.

يتتبع المكون "التحكم في التطبيق" الإجراءات التي يتم القيام بها في نظام التشغيل بواسطة التطبيقات المُثبَّتة على الكمبيوتر، كما أنه ينظمها وفقًا لقواعد. تقيد هذه القواعد نشاط التطبيقات المشتبه به، بما في ذلك وصول التطبيقات إلى الموارد المحمية، مثل الملفات والمجلدات، ومفاتيح السجلات، وعناوين الشبكة.

على أنظمة التشغيل 64 بت، لا يمكن تكوين حقوق التطبيقات للإجراءات التالية:

- الوصول المباشر إلى الذاكرة الفعلية
- إدارة برنامج تشغيل الطابعة
- إنشاء الخدمة
- قراءة الخدمة
- تحرير الخدمة
- إعادة تكوين الخدمة

- إدارة الخدمة
- بدء الخدمة
- إزالة الخدمة
- الوصول إلى بيانات المستعرض الداخلية
- الوصول إلى الكائنات الحرجة لنظام التشغيل
- الوصول إلى مخزن كلمات المرور
- إعداد حقوق مصحح الأخطاء
- استخدام واجهات البرامج لنظام التشغيل
- استخدام واجهات البرامج لنظام التشغيل (DNS)

على نظام التشغيل Microsoft Windows 8 64 بت، لا يمكن تكوين حقوق التطبيقات للإجراءات التالية:

- إرسال رسائل النوافذ إلى عمليات أخرى
- عمليات مشكوك فيها
- تثبيت برامج الاعتراض
- اعتراض أحداث التدفق الواردة
- أخذ لقطات الشاشة

يتم التحكم في نشاط التطبيق وفقًا مكون جدار الحماية.

عند تشغيل تطبيق على الكمبيوتر للمرة الأولى، يتحقق مكون التحكم في التطبيق من سلامة التطبيق ويقوم بتخصيصه لمجموعة (موثوق به أو غير موثوق به أو عالي التقييد أو منخفض التقييد). تقوم المجموعة الموثوقة بتعريف القواعد التي يجب أن يقوم برنامج Kaspersky Total Security بتطبيقها للتحكم في نشاط هذا التطبيق.

يمكنك تحرير قواعد التحكم في التطبيق يدويًا.

تكوين التحكم في التطبيق

لتكوين التحكم في التطبيقات:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.
3. في نافذة **الأدوات**، انقر فوق الرابط **التحكم في التطبيق** لفتح نافذة **التحكم في التطبيق**.
4. في نافذة **التحكم في التطبيق**، في القسم **التطبيقات**، انقر فوق الرابط **إدارة التطبيقات** لفتح نافذة **إدارة التطبيقات**.
5. في القائمة، حدد التطبيق المناسب وانقر نقرًا مزدوجًا فوقه لفتح النافذة **قواعد التطبيقات**.

   يتم فتح النافذة **قواعد التطبيقات**.

6. حدد قواعد التحكم في التطبيقات:

- لتكوين قواعد وصول تطبيق إلى موارد نظام التشغيل:
  a. من علامة التبويب **تسجيل النظام والملفات** حدد فئة المورد ذي الصلة.
  b. انقر بزر الماوس الأيمن فوق العمود الذي يحتوي على إجراء متوفر للمورد (**قراءة** أو **كتابة** أو **حذف** أو **إنشاء**) لفتح القائمة السياقية. في القائمة السياقية، حدد العنصر ذو الصلة (**سماح** أو **رفض** أو **المطالبة باتخاذ إجراء**).
- لتكوين حقوق التطبيق لتنفيذ إجراءات مختلفة في نظام التشغيل:
  a. من علامة التبويب **الحقوق** حدد فئة الحقوق ذات الصلة.
  b. انقر بزر الماوس الأيمن فوق عمود **الإذن** لفتح القائمة السياقية. في القائمة السياقية، حدد العنصر ذو الصلة (**سماح** أو **رفض** أو **المطالبة باتخاذ إجراء**).
- لتكوين حقوق التطبيق لتنفيذ إجراءات مختلفة على الشبكة:
  a. من علامة التبويب **قواعد الشبكة**، انقر فوق الزر **إضافة**.

     ستفتح النافذة **قاعدة الشبكة**.
  b. في النافذة التي ستفتح، حدد إعدادات القاعدة المطلوبة وانقر فوق **حفظ**.
  c. قم بتعيين أولوية للقاعدة الجديدة عن طريق النقر فوق الزرين **أعلى** و**أسفل** للانتقال لأعلى القائمة وأسفلها.
- لاستبعاد إجراءات محددة من قيود التحكم في التطبيق، من علامة التبويب **الاستثناءات** حدد خانات الاختيار الخاصة بالإجراءات التي لا تريد التحكم فيها.

7. انقر فوق الزر **حفظ**.

بالنسبة إلى كافة الاستثناءات التي تم إنشاؤها في قواعد التطبيقات، يمكن الوصول إليها في نافذة إعدادات التطبيق في القسم **التهديدات والاستثناءات**.

يقوم مكون التحكم في التطبيق بمراقبة وتقييد إجراءات التطبيق وفقًا للإعدادات المحددة.

تكوين وصول التطبيق إلى كاميرا الويب

قد يحاول المجرمون الحصول على وصول غير مصرح به إلى كاميرا الويب الخاصة بك عن طريق برنامج مخصص. يمنع Kaspersky Total Security الوصول غير المرخص إلى كاميرا الويب ويخطرك بمنع الوصول. وبشكل افتراضي، يمنع Kaspersky Total Security وصول التطبيقات المدرجة في مجموعة مقيد بشكل عالٍ أو غير موثوق به إلى كاميرا الويب.

يمكنك السماح للتطبيقات بالوصول إلى كاميرا الويب (انظر القسم "السماح للتطبيق بالوصول إلى كاميرا الويب" على صفحة 73) المضمنة في نافذة إعدادات مجموعات مستوى التقييد مرتفع والتحكم في التطبيق. إذا حاول أحد التطبيقات المدرجة في مجموعة "مقيد بشكل منخفض" الاتصال بكاميرا الويب، فسيعرض Kaspersky Total Security إخطارًا ويطالبك بتحديد ما إذا كنت تريد السماح لهذا التطبيق بالوصول إلى كاميرا الويب أم لا.

إذا تم إجراء محاولة الوصول إلى كاميرا الويب بواسطة تطبيق يتم رفض وصوله بشكل افتراضي، يعرض Kaspersky Total Security إخطارًا. يعرض الإخطار معلومات حول التأثير بأن التطبيق المثبت على الكمبيوتر (مثل Skype) يتلقى حاليًا بيانات الفيديو من كاميرا الويب. في قائمة الإخطارات المنسدلة، يمكنك منع التطبيق من الوصول إلى كاميرا الويب أو متابعة تكوين إعدادات وصول التطبيق إلى كاميرا الويب (انظر القسم "تكوين إعدادات وصول التطبيق إلى كاميرا الويب " على صفحة 73). لا يتم عرض هذا الإخطار إذا تم تشغيل التطبيق بالفعل في وضع ملء الشاشة على الكمبيوتر.

في القائمة المنسدلة حول بيانات الفيديو المستلمة بواسطة التطبيق، يمكنك أيضًا اختيار **إخفاء هذا الإخطار** أو متابعة تكوين إعدادات عرض الإخطار (راجع القسم "تكوين إعدادات وصول التطبيق إلى كاميرا الويب" على صفحة 73).

وبشكل افتراضي، يسمح Kaspersky Total Security لكاميرا الويب بالوصول إلى التطبيقات التي تطلب إذنك إذا كانت واجهة المستخدم الرسومية للتطبيق قيد التحميل أو تم تحميلها أو لا تستجيب، ويتعذر عليك الوصول يدويًا.

تحتوي حماية كاميرا الويب على المميزات والقيود التالية:

- يقيد Kaspersky Total Security الفيديو وتستمد الصور الثابتة من معالجة بيانات كاميرا الويب.
- يتحكم Kaspersky Total Security فقط في كاميرات الويب المتصلة عبر USB أو IEEE1394 التي تم عرضها في مدير جهاز Windows كأجهزة تصوير.

لعرض قائمة بكاميرات الويب المدعومة، انقر فوق هذا الرابط http://support.kaspersky.com/10978.

لتفعيل الحماية ضد الوصول غير المرخص لكاميرا الويب، يجب تمكين مكون التحكم في التطبيق.

تكوين إعدادات وصول التطبيق إلى كاميرا الويب

لتكوين إعدادات وصول التطبيق إلى كاميرا الويب:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **الإعدادات** لفتح نافذة **الإعدادات**.
3. في قسم **الحماية** في الجزء الأيمن من النافذة، حدد المكون **الوصول إلى كاميرا الويب**.
4. تكوين إعدادات الوصول إلى كاميرا ويب الكمبيوتر:
   - لمنع جميع التطبيقات من الوصول إلى كاميرا الويب، حدد خانة الاختيار **منع الوصول إلى كاميرا الويب لكل التطبيقات**.
   - لاستلام إخطارات عند استخدام كاميرا الويب بواسطة تطبيق غير مسموح له بذلك، حدد خانة الاختيار **إظهار إخطار عند استخدام كاميرا الويب بواسطة تطبيق يُسمح له باستخدام كاميرا الويب**.
   - لسماح وصول جميع التطبيقات إلى كاميرا الويب، في نافذة **الإعدادات** في علامة تبويب **الحماية** قم بتعطيل **الوصول إلى كاميرا الويب**.

السماح بوصول التطبيق إلى كاميرا الويب

للسماح لتطبيق بالوصول إلى كاميرا الويب:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.
3. في نافذة **الأدوات**، انقر فوق الرابط **التحكم في التطبيق** لفتح نافذة **التحكم في التطبيق**.
4. في نافذة **التحكم في التطبيق**، في القسم **التطبيقات**، انقر فوق الرابط **إدارة التطبيقات** لفتح نافذة **إدارة التطبيقات**.
5. في القائمة، حدد التطبيق الذي تريد السماح له بالوصول إلى كاميرا الويب. انقر نقرًا مزدوجًا فوق التطبيق لفتح نافذة **قواعد التطبيقات**.
6. في نافذة **قواعد التطبيقات** انتقل إلى علامة التبويب **الحقوق**.

7. في قائمة فئات الحقوق، حدد **تعديل النظام** **تعديلات نظام مشكوك فيها** **الوصول إلى كاميرا الويب**.
8. انقر بزر الماوس الأيمن فوق العمود **الإذن** لفتح القائمة السياقية وحدد **سماح**.
9. انقر فوق الزر **حفظ**.

سيتم السماح للتطبيق المحدد بالوصول إلى كاميرا الويب.

وضع التطبيقات الموثوقة

يوفر هذا القسم معلومات حول وضع التطبيقات الموثوق بها.

في هذا القسم

حول وضع التطبيقات الموثوق بها

في Kaspersky Total Security، يمكنك إنشاء بيئة آمنة على الكمبيوتر الخاص بك، تُسمى وضع التطبيقات الموثوق بها، حيث يسمح فقط بتشغيل التطبيقات الموثوق بها. سيكون وضع التطبيقات الموثوق بها مفيدًا لك إذا كنت تستخدم مجموعة ثابتة من التطبيقات المعروفة ولا تحتاج بشكل متكرر إلى تشغيل تطبيقات جديدة وغير معروفة يتم تنزيلها من الإنترنت. عند التشغيل في وضع التطبيقات الموثوق بها، يقوم Kaspersky Total Security بحظر جميع التطبيقات التي لم يتم تصنيفها على أنها موثوق بها بواسطة Kaspersky Lab. يعتمد قرار ما إذا سيتم الوثوق في تطبيق أم لا على المعلومات المستلمة من شبكة اتصال أمان Kaspersky وتفاصيل التوقيع الرقمي للتطبيق ومستوى ثقة المثبت ومصدر تنزيل التطبيق.

يحتوي وضع التطبيقات الموثوق بها على المزايا والقيود التالية:

- لاستخدام وضع التطبيقات الموثوق بها، تأكد من تمكين جميع مكونات الحماية التالية: التحكم في التطبيق ومكافحة فيروسات الملفات ومراقب النظام. في حالة توقف تشغيل أي من هذه المكونات، يتم تعطيل وضع "التطبيقات الموثوق بها".
- وقد لا يتوفر وضع التطبيقات الموثوق بها إذا كانت ملفات النظام موجودة على أقسام محرك الأقراص الثابت مع نظام ملف غير NTFS.
- ربما يكون وضع "التطبيقات الموثوق بها" غير موجود أو غير متاح في الإصدار الحالي من Kaspersky Total Security. يعتمد توفر التطبيقات الموثوق بها في Kaspersky Total Security على المنطقة وموفر الخدمة. إذا كنت تحتاج إلى وضع التطبيقات الموثوق بها، فنوصيك بطلبه عند شراء التطبيق.
- إذا تم دعم وضع التطبيقات الموثوق بها في إصدار Kaspersky Total Security الخاص بك لكنه غير متوفر حاليًا، فربما يصبح متوفرًا بعد تحديث قواعد البيانات ووحدات البرنامج النمطية (انظر القسم "تحديث قواعد البيانات ووحدات البرنامج النمطية" على صفحة 36). بعد تحديث قواعد البيانات ووحدات التطبيق البرمجية، يمكنك تكوين وضع التشغيل للتطبيقات والوحدات غير المعروفة.

قبل تمكين وضع "التطبيقات الموثوق بها"، يحلل Kaspersky Total Security نظام التشغيل والتطبيقات المُثبَّتة على الكمبيوتر. قد يستغرق التطبيق وقتًا طويلاً (قد يصل إلى بضع ساعات). إذا اكتشف التحليل برامج لا يمكن تصنيفها كموثوق بها، فلا نوصيك بتمكين وضع "التطبيقات الموثوق بها". عند تمكين وضع التطبيقات الموثوق بها، قد يمنع Kaspersky Total Security التطبيقات التي لم يتم الاعتراف بها على أنها موثوقة. يمكنك السماح بتشغيل هذه التطبيقات (انظر القسم "التحكم في أنشطة التطبيقات الموجودة على الكمبيوتر والشبكة" على صفحة 70) إذا كنت تستخدم إحداها ثم قمت بتمكين وضع التطبيقات الموثوق بها.

يمكن لـ Kaspersky Total Security إجراء تحليل لنظام التشغيل والتطبيقات المثبتة تلقائيًا في الخلفية. إذا أظهر التطبيق الذي تم إجراؤه بواسطة Kaspersky Total Security أن التطبيقات الموثوق بها مستخدمة على الكمبيوتر، فربما يتم تمكين وضع التطبيقات الموثوق بها تلقائيًا.

تمكين الوضع "تطبيقات موثوقة"

لتمكين الوضع "تطبيقات موثوقة":

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.
3. في نافذة **الأدوات**، انقر فوق الرابط **التحكم في التطبيق** لفتح نافذة **التحكم في التطبيق**.
4. في الجزء السفلي من النافذة، في القسم **تم تعطيل وضع التطبيقات الموثوقة** بنافذة **التحكم في التطبيق**، انقر فوق الرابط **تمكين**.

   في حالة تعطيل مكونات الحماية المطلوبة، يتم فتح نافذة توفر معلومات حول مكونات الحماية التي يجب تمكينها قبل تمكين وضع التطبيقات الموثوق بها.

5. انقر فوق الزر **متابعة**.

   يقوم هذا بتشغيل تحليل نظام التشغيل والتطبيقات المثبتة باستثناء الملفات المؤقتة ومكتبات الرابط الديناميكي للمصدر الذي يحتوي على الرمز القابل للتنفيذ. يتم عرض تقدم عملية التحليل في النافذة **تحليل التطبيقات المُثبَّتة** التي يتم فتحها.

   انتظر حتى انتهاء تحليل نظام التشغيل والتطبيقات المثبتة. يمكنك تصغير النافذة **تحليل التطبيقات المُثبَّتة**. يتم إجراء التحليل في وضع الخلفية. يمكنك عرض تقدم التحليل عبر النقر فوق رابط **تحليل التطبيقات المُثبَّتة** (<N> %) في نافذة **التحكم في التطبيق**.

6. يمكنك عرض معلومات حول نتائج التحليل في **نافذة** اكتمل تحليل التطبيقات المثبتة والملفات القابلة للتنفيذ.

   إذا تم اكتشاف ملفات نظام ذات خصائص غير محددة أثناء التحليل، فنوصيك بتجنب تمكين وضع "التطبيقات الموثوق بها". ونوصيك أيضًا بتجنب تمكين وضع التطبيقات الموثوق بها إذا تم اكتشاف العديد من التطبيقات، والتي لا يمتلك Kaspersky Total Security معلومات كافية لها لتصنيفها كآمنة تمامًا.

   يمكنك عرض معلومات حول ملفات النظام غير المعروفة بالنقر فوق الرابط **الانتقال إلى قائمة ملفات النظام غير المعروفة**. يتم عرض قائمة ملفات النظام غير المعروفة في النافذة **ملفات نظام غير معروفة**. يمكنك أيضًا إلغاء استخدام الوضع "التطبيقات الموثوق بها" بالنقر فوق الزر **لا تقم بتمكين وضع التطبيقات الموثوقة**.

7. إذا كنت ترغب في السماح بتشغيل التطبيقات وملفات النظام غير الموثوق بها، ففي نافذة **اكتمل تحليل التطبيقات المُثبَّتة والملفات القابلة للتنفيذ**، انقر فوق رابط **السماح بتشغيل ملفات النظام غير المعروفة والمتابعة**.
8. انقر فوق الزر **تمكين وضع التطبيقات الموثوقة بشكل افتراضي**.

تم الآن تمكين وضع التطبيقات الموثوق بها. سيمنع Kaspersky Total Security جميع التطبيقات وملفات النظام التي لم يتم تصنيفها كموثوق بها. ينتقل التطبيق إلى النافذة **التحكم في التطبيق**.

بعد تمكين وضع التطبيقات الموثوق بها وإعادة تشغيل نظام التشغيل لأول مرة، يتم السماح بتشغيل التطبيقات غير المعروفة حتى يتم تشغيل Kaspersky Total Security. وبعد إعادة تشغيل نظام التشغيل، يقوم Kaspersky Total Security بمنع تشغيل التطبيقات غير المعروفة.

تعطيل وضع "التطبيقات الموثوق بها"

لتعطيل الوضع "تطبيقات موثوقة":

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.
3. في نافذة **الأدوات**، انقر فوق الرابط **التحكم في التطبيق** لفتح نافذة **التحكم في التطبيق**.
4. في الجزء السفلي من النافذة، في القسم **تم تمكين وضع التطبيقات الموثوقة**، انقر فوق الرابط **تعطيل**.

تم الآن تعطيل وضع التطبيقات الموثوق بها.

أداة التخلص من الملفات

يمكنك ضمان الحصول على حماية إضافية للبيانات الشخصية عن طريق حماية البيانات المحذوفة ضد الاستعادة غير المصرح بها بواسطة المهاجمين.

يحتوي Kaspersky Total Security على أداة للحذف النهائي للبيانات التي تجعل استعادة البيانات باستخدام أدوات البرامج القياسية أمرًا مستحيلاً.

يجعل Kaspersky Total Security من الممكن أن يتم حذف البيانات بدون احتمال استعادتها من وسيط البيانات التالي:

- محركات أقراص الشبكة والمحلية. يكون الحذف ممكنًا إذا كان لديك الحقوق اللازمة لكتابة البيانات وحذفها.
- المحركات القابلة للإزالة أو الأجهزة الأخرى التي يمكن كشفها كمحركات قابلة للإزالة (مثل الأقراص المرنة أو بطاقات الفلاش أو أقراص USB أو الهواتف الخلوية). ويمكن حذف البيانات من بطاقة ذاكرة فلاش إذا كانت الحماية الميكانيكية من إعادة الكتابة معطلة.

يمكنك حذف البيانات التي يمكنك الوصول إليها في حسابك الشخصي. قبل حذف البيانات ، تأكد من أنها غير مستخدمة بواسطة التطبيقات الموجودة قيد التشغيل.

لحذف البيانات نهائيًا:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.

3. في نافذة **الأدوات**، انقر فوق الرابط **أداة تمزيق الملفات** لفتح نافذة **أداة تمزيق الملفات** (راجع الشكل أدناه).



الشكل *6*. **نافذة** أداة التخلص من الملفات

4. انقر فوق الزر **استعراض**، وفي نافذة **تحديد مجلد** التي تفتح، حدد المجلد أو الملف الذي تريد حذفه نهائيًا.

قد يتسبب حذف ملفات ومجلدات النظام في أن يعمل نظام التشغيل بشكل غير سليم.

5. من القائمة المنسدلة **طريقة حذف البيانات**، حدد الخوارزمية المطلوبة لحذف البيانات.

لحذف البيانات من أجهزة SSD وUSB، إلى جانب محركات الأقراص على الشبكة، يوصى بتطبيق **الحذف السريع** أو **طريقة** GOST R 50739-95. قد تؤدي طرق الحذف الأخرى إلى الحاق الضرر بجهاز SSD أو USB أو محرك أقراص الشبكة.

6. انقر فوق الزر **إزالة**.

7. في نافذة تأكيد الحذف التي تفتح، انقر فوق **نعم**. إذا لم يتم حذف بعض الملفات، حاول مرة أخرى القيام بحذفها بالنقر على الزر **إعادة المحاولة** في النافذة التي ستفتح. لتحديد مجلد آخر لحذفه، انقر الزر **إنهاء**.

النسخ الاحتياطي والاستعادة

يوفر هذا القسم معلومات حول النسخ الاحتياطي للبيانات.

في هذا القسم

حول النسخ الاحتياطي والاستعادة

يُعد نسخ البيانات ضروري لحماية بياناتك من الفقدان عند حدوث خلل بالكمبيوتر أو سرقته، أو عند حذفها بدون قصد أو إفسادها بواسطة القراصنة .

لنسخ البيانات احتياطيًا، قم بإنشاء (راجع القسم "إنشاء مهمة نسخ احتياطي" على صفحة 80) وابدأ (انظر القسم "بدء مهمة نسخ احتياطي" على صفحة 83) مهمة نسخ احتياطي. يمكن بدء تشغيل المهمة تلقائيًا وفقًا للجدول أو يدويًا. يتيح لك التطبيق أيضًا عرض معلومات حول مهام النسخ الاحتياطي المكتملة.

يوصى بحفظ نسخ البيانات الاحتياطية على محركات الأقراص القابلة للإزالة أو في مخزن متاح عبر الإنترنت.

يمكنك Kaspersky Total Security استخدام أنواع التخزين التالية لإنشاء النُسخ الاحتياطية:

- محرك الأقراص المحلي
- محرك الأقراص القابل للإزالة (مثل محرك أقراص صلبة خارجي)
- محرك أقراص الشبكة
- خادم FTP
- المخزن المتاح عبر الإنترنت (راجع القسم "حول المخزن المتاح عبر الإنترنت" على صفحة 84).

إنشاء مهمة نسخ احتياطي

لإنشاء مهمة نسخ احتياطي:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق زر **النسخ الاحتياطي والاستعادة**.

3. في نافذة **النسخ الاحتياطي والاستعادة** التي ستفتح، قم بتنفيذ العمليات التالية:

- انقر فوق الزر **حدد ملفات للنسخ الاحتياطي** إذا لم يتم إنشاء مهمة نسخ احتياطي بعد
- انقر فوق الزر **إنشاء نُسخ احتياطية لملفات أخرى** إذا كان لديك بالفعل مهمة نسخ احتياطي وترغب في إنشاء مهمة جديدة.

سيتم بدء تشغيل معالج إنشاء مهمة النسخ الاحتياطي.

يتكون "المعالج" من سلسلة من الصفحات (الخطوات) التي يمكنك التنقل بينها بالنقر فوق الزرين **رجوع** و**التالي**. لإغلاق "المعالج" بعد انتهائه، انقر فوق الزر **إنهاء**. لإيقاف المعالج في أي مرحلة، انقر الزر **إلغاء**.

دعنا نقوم بمراجعة خطوات المعالج بقدر أكبر من التفصيل.

تحديد نوع البيانات

في هذه الخطوة من المعالج، حدد نوع البيانات أو حدد المجلدات التي ترغب في نسخها احتياطيًا:

- حدد أحد أنواع البيانات سابقة التعيين (الملفات من مجلدات "مستنداتي" و"سطح المكتب"، والصور ومقاطع الفيديو، والصور، وملفات الموسيقى) لإجراء التكوين السريع.
- حدد الخيار **إنشاء نُسخ احتياطية للملفات في المجلدات المحددة** لتحديد الملفات والمجلدات التي تريد نسخها احتياطيًا.

تحديد مجلدات للنسخ الاحتياطي

إذا قمت بتحديد الخيار **إنشاء نُسخ احتياطية للملفات في المجلدات المحددة** في الخطوة السابقة من المعالج، فانقر فوق الزر **إضافة مجلد** وحدد مجلدًا في النافذة **تحديد ملف أو مجلد** التي تفتح أو اسحب المجلد إلى نافذة التطبيق.

حدد خانة الاختيار **تحديد أنواع الملفات أيضًا** إذا كنت تريد تحديد فئات الملفات التي سيتم نسخها احتياطيًا في المجلدات المحددة.

حدد فئات الملفات للنسخ الاحتياطي

إذا قمت بتحديد خانة الاختيار **تحديد أنواع الملفات أيضًا** في الخطوة السابقة من المعالج، ففي النافذة التالية حدد خانات الاختيار المقابلة لفئات الملفات التي تريد نسخها احتياطيًا.

تحديد التخزين

في هذه الخطوة، حدد مخزن النسخ الاحتياطي:

- **التخزين على الإنترنت**. حدد هذا الخيار إذا كنت تريد تخزين النُسخ الاحتياطية على مخزن متاح عبر الإنترنت. قبل استخدام المخزن المتاح عبر الإنترنت، يتطلب منك تفعيل المخزن المتاح عبر الإنترنت (انظر القسم "تفعيل المخزن المتاح عبر الإنترنت" على صفحة 84). عند نسخ البيانات في مخزن الإنترنت بشكل احتياطي، لا يقوم Kaspersky Total Security بإنشاء نُسخ احتياطية من البيانات التي تخضع أنواعها للقيود التي تفرضها قواعد استخدام Dropbox.
- **محرك الأقراص المحلي (:C)**. حدد هذا الخيار إذا كنت تريد تخزين النُسخ الاحتياطية على محرك أقراص محلي.
- **مخزن الشبكة**. إذا كنت ترغب في تخزين النُسخ الاحتياطية في مخزن شبكة، فحدد مخزن الشبكة المعني في القائمة.
- **محرك أقراص قابل للإزالة**. إذا كنت ترغب في تخزين النُسخ الاحتياطية على محرك أقراص قابل للإزالة، فحدد محرك الأقراص القابل للإزالة المعني في القائمة.

لضمان أمان البيانات، نوصي بإنشاء مخزن الإنترنت أو مخازن النسخ الاحتياطي على محركات أقراص قابلة للإزالة.

➡ *لإضافة مخزن شبكة:*

1. انقر فوق الرابط **إضافة مخزن شبكي** لفتح نافذة **إضافة مخزن شبكي** وحدد نوع المخزن الشبكي: محرك أقراص الشبكة أو خادم FTP.
2. حدد البيانات المطلوبة للاتصال بمخزن الشبكة.
3. انقر فوق **موافق**.

➡ *لإضافة محرك أقراص قابل للإزالة كمخزن نسخ احتياطي:*

1. انقر فوق الرابط **الاتصال بمخزن موجود** لفتح نافذة **توصيل المخزن**.
2. حدد القسم **محرك الأقراص القابل للإزالة**.
3. انقر فوق الزر **استعراض**، وفي النافذة التي تفتح حدد القرص القابل للإزالة الذي تريد حفظ نسخ الملفات الاحتياطية عليه.

حدد خانة الاختيار **استخدام الإعدادات الممتدة للتخزين** لتكوين إعدادات تخزين الملف مثل عدد إصدارات الملف المخزنة ومدة تخزين النسخ الاحتياطية.

إنشاء الجدول الزمني للنسخ الاحتياطي

قم بإجراء واحدة مما يلي في هذه الخطوة من المعالج:

- حدد جدول مهمة النسخ الاحتياطي إذا كنت ترغب في بدء مهمة النسخ الاحتياطي تلقائيًا.
- في قائمة **تشغيل النسخ الاحتياطي** حدد الخيار **يدويًا** إذا كنت ترغب فب بدء المهمة يدويًا.

تعيين كلمة مرور لحماية النُسخ الاحتياطية

حدد خانة الاختيار **تمكين الحماية بكلمة مرور** وقم بتعبئة الحقول **كلمة مرور الوصول إلى النُسخ الاحتياطية** و**تأكيد كلمة المرور** لحماية الوصول إلى النُسخ الاحتياطية باستخدام كلمة مرور.

إعدادات تخزين الملفات

تتوفر هذه الخطوة إذا تم تحديد خانة الاختيار **استخدام الإعدادات الممتدة للتخزين** في الخطوة السابقة.

تكوين إعدادات تخزين الملفات:

- حدد خانة الاختيار **تقييد عدد نسخ الملف** وفي القائمة **النسخ التي سيتم تخزينها** حدد عدد نسخ ملف واحد سيتم تخزينه.
- حدد خانة الاختيار **تقييد فترة تخزين نسخ الملف** وفي القائمة **الاحتفاظ بالنسخ الأقدم من الملفات لمدة** حدد عدد الأيام التي ينبغي تخزين كل نسخة ملف فيها.

إدخال اسم مهمة النسخ الاحتياطي

قم بإجراء ما يلي في هذه الخطوة:

1. أدخل اسم مهمة النسخ الاحتياطي.
2. حدد خانة الاختيار **تشغيل النسخ الاحتياطي بمجرد اكتمال المعالج** لبدء عملية النسخ الاحتياطي عند انتهاء المعالج.

اكتمال المعالج

انقر فوق زر **إنهاء**.

يتم إنشاء مهمة نسخ احتياطي. تظهر المهمة التي قمت بإنشائها في نافذة **النسخ الاحتياطي والاستعادة**.

بدء مهمة نسخ احتياطي

لبدء مهمة نسخ احتياطي:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق زر **النسخ الاحتياطي والاستعادة**.
3. في نافذة **النسخ الاحتياطي والاستعادة** التي تفتح، حدد مهمة نسخ احتياطي وانقر فوق الزر **تشغيل النسخ الاحتياطي**.

   يتم بدء تشغيل مهمة نسخ احتياطي.

استعادة البيانات من النسخ الاحتياطي

لاستعادة البيانات من النسخ الاحتياطي:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق زر **النسخ الاحتياطي والاستعادة**.
3. قم بإجراء أيّ مما يلي:
   - انقر فوق الزر **استعادة الملفات** المقابل لمهمة النسخ الاحتياطي ذات الصلة.
   - انقر فوق الزر **إدارة المخازن** لفتح نافذة وانقر فوق الزر **استعادة الملفات** المقابل لمخزن النسخ الاحتياطي ذي الصلة.
4. في القائمة المنسدلة **تاريخ النسخ الاحتياطي** حدد تاريخ إنشاء نسخة احتياطية.
5. حدد خانات الاختيار المقابلة للمجلدات التي تريد استعادتها.
6. لاستعادة فئات محددة من الملفات، حدد هذه الفئات في قائمة نوع الملف المنسدلة.
7. انقر فوق زر **استعادة الملفات المحددة**.

   يتم فتح النافذة **استعادة البيانات من النسخ الاحتياطي**.
8. حدد أحد الخيارين التاليين:
   - **المجلد المصدر**. إذا تم تحديد هذا الخيار، فيقوم التطبيق باستعادة البيانات إلى المجلد المصدر.
   - **المجلد المحدد**. إذا تم تحديد هذا الخيار، فيقوم التطبيق باستعادة البيانات إلى المجلد المحدد. انقر فوق الزر **استعراض** لتحديد المجلد الذي تريد استعادة البيانات إليه.
9. في القائمة المنسدلة **في حالة تعارض أسماء**، حدد الإجراء الذي سيتم تنفيذه بواسطة التطبيق عندما يكون اسم الملف الذي يتم استعادته مطبقًا لاسم الملف الموجود بالفعل في مجلد الوجهة.
10. انقر فوق الزر **استعادة**.

ستتم استعادة الملفات المحددة للاسترداد من النسخ الاحتياطي وحفظها في المجلد المحدد.

حول المخزن المتاح عبر الإنترنت

يتيح لك Kaspersky Total Security حفظ نُسخ احتياطية من بياناتك على خادم بعيد عبر خدمة Dropbox.

لاستخدام المخزن المتاح عبر الإنترنت:

- تأكد من اتصال الكمبيوتر بالإنترنت.
- قم بإنشاء حساب على موقع ويب موفر خدمة تخزين البيانات عبر الإنترنت.
- قم بتفعيل المخزن المتاح عبر الإنترنت.

يمكنك استخدام حساب Dropbox واحد لإجراء النسخ الاحتياطي للبيانات من أجهزة مختلفة مُثبت عليها برنامج Kaspersky Total Security إلى مخزن إنترنت واحد.

يتم تحديد حجم المخزن المتاح عبر الإنترنت بواسطة موفر خدمات التخزين عبر الإنترنت، خدمة ويب Dropbox. راجع موقع ويبDropbox https://www.dropbox.com لمزيد من التفاصيل حول بنود استخدام خدمة الويب.

تفعيل المخزن المتاح عبر الإنترنت

تنشيط التخزين على الإنترنت:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق زر **النسخ الاحتياطي والاستعادة**.
3. في نافذة **النسخ الاحتياطي والاستعادة** التي ستفتح، قم بتنفيذ العمليات التالية:
   - انقر فوق الزر **حدد ملفات للنسخ الاحتياطي** إذا لم يتم إنشاء مهمة نسخ احتياطي سابقًا.
   - انقر فوق الزر **إنشاء نُسخ احتياطية لملفات أخرى** إذا كان لديك مهمة نسخ احتياطي بالفعل.

   يتم بدء تشغيل معالج إنشاء مهمة نسخ احتياطي (انظر القسم "إنشاء مهمة نسخ احتياطي" على صفحة 80).
4. في نافذة تحديد نوع البيانات، حدد فئة البيانات أو حدد يدويًا الملفات التي تريد نسخها احتياطيًا.
5. في نافذة تحديد التخزين، حدد التخزين على الإنترنت، وانقر فوق زر **تفعيل**.

   ويلزم توفر اتصال بالإنترنت لإنشاء مخزن متاح عبر الإنترنت.

   يتم فتح مربع حوار لتسجيل الدخول إلى حساب Dropbox.
6. في النافذة التي يتم فتحها، قم بإحدى العمليات التالية:
   - أكمل التسجيل إذا لم تكن مستخدم Dropbox مسجلاً.
   - إذا كنت مستخدم Dropbox مسجلاً، فقم بتسجيل الدخول إلى حسابك على Dropbox.
7. لإنهاء عملية تنشيط وظيفة التخزين على الإنترنت، تأكد من السماح باستخدام برنامج Kaspersky Total Security لحسابك على Dropbox لنسخ البيانات احتياطيًا واستعادتها. يضع Kaspersky Total Security نُسخًا احتياطية من البيانات المحفوظة في مجلد منفصل يتم إنشاؤه في مجلد تخزين Dropbox للتطبيقات.

بعد اكتمال عملية تنشيط وظيفة التخزين على الإنترنت، يتم فتح نافذة تحديد المخزن. وهي تتضمن مجموعة من مخازن الإنترنت لتختار منها. بالنسبة لوظيفة التخزين على الإنترنت التي تم تنشيطها، يعرض التطبيق حجم المساحة المستخدمة وحجم المساحة المتاحة لتخزين البيانات.

تخزين البيانات في مخازن البيانات

يوضح هذا القسم كيفية حماية البيانات باستخدام مخازن البيانات.

في هذا القسم

حول مخزن البيانات

تم تصميم مخازن البيانات لحماية البيانات السرية ضد الوصول غير المصرح به. *مخزن البيانات* هو مخزن على الكمبيوتر يمكنك قفله أو إلغاء قفله باستخدام كلمة مرور تعرفها أنت فقط. يتطلب منك إدخال كلمة المرور لتعديل الملفات المخزنة في مخزن بيانات مقفل.

إذا فقدت كلمة المرور أو نسيتها، فلن تتمكن من استعادة بياناتك.

يستخدم Kaspersky Total Security خوارزميات تشفير البيانات التالية لإنشاء مخازن البيانات: AES XTS 256 وDRBG-SHA2-256 وPBKDF-SHA2-256.

نقل الملفات إلى مخزن البيانات

لوضع الملفات في مخزن البيانات:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الزر **تشفير البيانات**.
3. في النافذة **تشفير البيانات** التي يتم فتحها، قم بتنفيذ أي مما يلي:
   - انقر فوق الزر **إنشاء مخزن بيانات جديد** إذا كنت لا تمتلك مخزن بيانات بالفعل.
   - انقر فوق الزر **إنشاء مخزن بيانات** إذا قمت بإنشاء مخزن بيانات سابقًا.
4. انقر فوق الزر **إضافة ملفات ومجلدات إلى مخزن بيانات** لفتح Explorer وحدد الملفات التي تريد وضعها في مخزن البيانات.

   تظهر الملفات المحددة في نافذة **تشفير البيانات**.
5. انقر فوق الزر **متابعة**.
6. أدخل اسم مخزن البيانات وحدد مكانه أو استخدم قيم افتراضية لهذه الإعدادات.
7. لكي تتمكن من الوصول إلى مخزن البيانات سريعًا، حدد خانة الاختيار **إنشاء اختصار على سطح المكتب لمخزن البيانات**.

8. انقر فوق الزر **متابعة**.
9. قم بتعبئة حقول **كلمة المرور** و**تأكيد كلمة المرور** وانقر فوق **متابعة**.
10. حدد ما تريد فعله مع نسخ الملفات الأصلية خارج مخزن البيانات:
    - لحذف نسخ ملفات أصلية خارج مخزن البيانات، انقر فوق **إزالة**.
    - لحفظ نسخ ملفات أصلية خارج مخزن البيانات، انقر فوق **تخطي**.
11. انقر فوق زر **إنهاء**.

    يظهر مخزن البيانات الذي قمت بإنشائه في قائمة **مخازن بياناتك**.
12. لقفل مخزن البيانات، انقر فوق الزر **قفل مخزن البيانات**.

    تصبح البيانات الموجودة في مخزن بيانات مقفل متوفرة فقط بعد إدخال كلمة مرور.

الوصول إلى الملفات المخزنة في مخزن البيانات

للوصول إلى البيانات الموجودة في مخزن بيانات:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الزر **تشفير البيانات**.
3. في نافذة **تشفير البيانات** التي تفتح، انقر فوق الزر **فتح مخزن البيانات** المجاور لمخزن البيانات الذي تحتاجه.
4. أدخل كلمة المرور وانقر فوق الزر **فتح مخزن البيانات في Windows Explorer**.

تظهر الملفات المخزنة في مخزن البيانات في نافذة Explorer. يمكنك إجراء التغييرات الضرورية على الملفات وقفل مخزن البيانات مرة أخرى.

لإلغاء قفل مخازن البيانات التي تم إنشاؤها باستخدام إصدار سابق للتطبيق، قم بتحويل تنسيق مخزن البيانات القديم إلى التنسيق الجديد. يطالبك التطبيق بإجراء المحادثة عند محاولة فتح مخزن بيانات في Kaspersky Total Security.

يمكن أن يستغرق تحويل محادثة مخزن بيانات إلى التنسيق الجديد فترة طويلة بناءً على حجم مخزن البيانات.

الوصول المحمي بكلمة المرور إلى خيارات إدارة KASPERSKY TOTAL SECURITY

يمكن مشاركة كمبيوتر واحد بواسطة مستخدمين متعددين يمتلكون مستويات مختلفة من الخبرة والمعرفة بالكمبيوتر. قد يؤدي الوصول غير المقيد بواسطة عدة مستخدمين مختلفين إلى Kaspersky Total Security وإعداداته إلى تعريض مستوى أمان الكمبيوتر للخطر.

لتقييد الوصول إلى التطبيق، يمكنك تعيين كلمة مرور المسؤول وتحديد الإجراءات التي ينبغي أن تطلب إدخال كلمة المرور هذه:

- تكوين إعدادات التطبيق.
- إيقاف التطبيق.
- إزالة التطبيق.

للوصول المحمي بكلمة مرور للتحكم في Kaspersky Total Security:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **الإعدادات** للانتقال إلى قسم **الإعدادات**.
3. في الجزء الأيمن من النافذة، حدد القسم **عام**، وانقر فوق الرابط **إعداد الحماية بكلمة مرور** لفتح النافذة **الحماية بكلمة مرور**.
4. في النافذة التي يتم فتحها، املأ الحقلين **كلمة المرور الجديدة** و**تأكيد كلمة المرور**.
5. في مجموعة إعدادات **نطاق كلمة المرور**، حدد إجراءات التطبيق التي تريد تقييد الوصول إليها.

لا يمكن استعادة كلمة مرور منسية. إذا نسيت كلمة المرور، فاتصل بقسم "الدعم الفني" لاسترداد إمكانية الوصول إلى إعدادات Kaspersky Total Security.

إيقاف حماية الكمبيوتر واستعادتها

يعني الإيقاف المؤقت للحماية التعطيل المؤقت لجميع مكونات الحماية لبعض الوقت.

عند إيقاف الحماية مؤقتًا أو عدم تشغيل Kaspersky Total Security، تتم مراقبة نشاط التطبيقات التي يتم تشغيلها على الكمبيوتر الخاص بك. يتم حفظ معلومات حول نتائج مراقبة نشاط التطبيق في نظام التشغيل. عند بدء تشغيل Kaspersky Total Security مرة أخرى أو عند استئناف الحماية، يستخدم Kaspersky Total Security هذه المعلومات لحماية الكمبيوتر من الأنشطة الخبيثة التي قد يتم تنفيذها عند توقف الحماية مؤقتًا أو عند عدم تشغيل Kaspersky Total Security. يتم تخزين معلومات حول نتائج مراقبة نشاط التطبيق بشكل غير محدود. يتم حذف هذه المعلومات في حالة إزالة Kaspersky Total Security من الكمبيوتر.

➡ *لإيقاف حماية الكمبيوتر مؤقتًا:*

1. في منطقة الإخطارات بشريط المهام، في القائمة السياقية لرمز التطبيق، حدد **إيقاف الحماية مؤقتًا**.

   يتم فتح النافذة **إيقاف الحماية مؤقتًا** (راجع الشكل التالي).



الشكل 7. النافذة إيقاف الحماية مؤقتًا

2. في النافذة **إيقاف الحماية مؤقتًا**، حدد الفترة الزمنية التي ينبغي استئناف الحماية بعد انقضائها:

   - **إيقاف مؤقت لفترة محددة** – سيتم تمكين الحماية بعد انتهاء الفاصل الزمني المحدد من القائمة المنسدلة.
   - **إيقاف مؤقت حتى إعادة التشغيل** – سيتم تمكين الحماية بعد إعادة تشغيل التطبيق مرة أخرى أو إعادة تشغيل نظام التشغيل (إذا تم تشغيل التطبيق تلقائيًا عند بدء التشغيل).
   - **إيقاف مؤقت** – سيتم استئناف الحماية بعد أن تقرر أنت استئنافها.

➡ *لاستئناف حماية الكمبيوتر:*

في منطقة الإخطارات بشريط المهام، في القائمة السياقية لرمز التطبيق، حدد **استئناف الحماية**.

استعادة إعدادات التطبيق الافتراضية.

يمكنك استعادة الإعدادات التي توصي بها Kaspersky Lab لبرنامج Kaspersky Total Security في أي وقت تريد. يمكن استعادة الإعدادات باستخدام *"معالج تكوين التطبيق"* .

عندما يكمل "المعالج" عملياته، يتم تعيين مستوى الأمان *موصى به* لجميع مكونات الحماية. عند استعادة مستوى الأمان المستحسن، يمكنك حفظ قيم الإعدادات المحددة سابقًا لمكونات التطبيق.

لتشغيل معالج تكوين التطبيق:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الإعدادات**.

   تعرض النافذة القسم **الإعدادات**.
3. حدد القسم **عام**.

   تعرض النافذة إعدادات Kaspersky Total Security.
4. في الجزء السفلي من النافذة، في القائمة المنسدلة **إدارة الإعدادات** حدد **استعادة الإعدادات**.

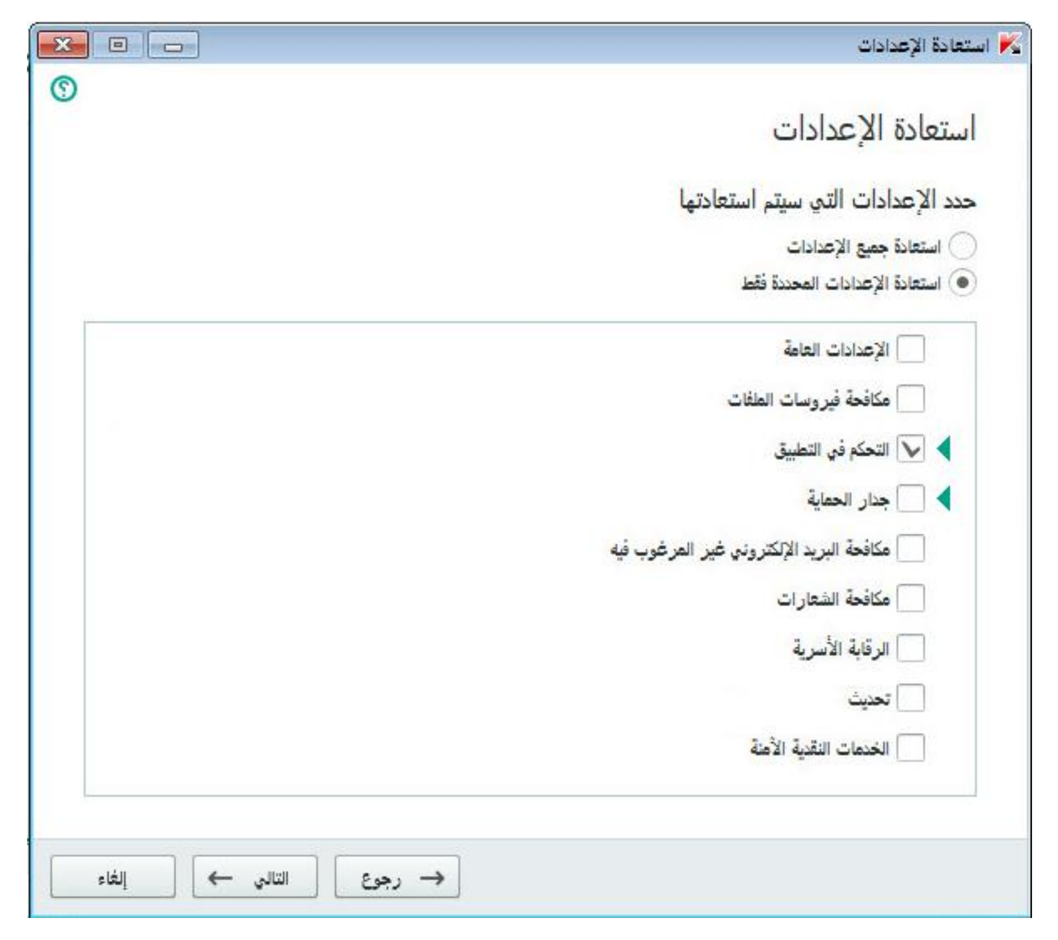
دعنا نقوم بمراجعة خطوات المعالج بقدر أكبر من التفصيل.

الخطوة 1. بدء تشغيل المعالج

انقر الزر **التالي** لمتابعة التثبيت.

الخطوة 2. استعادة الإعدادات

تعرض نافذة "المعالج" هذه مكونات حماية Kaspersky Total Security التي لها إعدادات مختلفة عن القيمة الافتراضية نظرًا لأنه تم تغييرها بواسطة المستخدم أو تجميعها بواسطة Kaspersky Total Security خلال التدريب ("جدار الحماية" أو "مكافحة البريد الإلكتروني غير المرغوب فيه"). في حالة إنشاء إعدادات خاصة لأي من المكونات، سيتم إظهارها أيضًا في النافذة (راجع الشكل التالي).



الشكل 8. النافذة استعادة الإعدادات

تشتمل الإعدادات الخاصة على قوائم بالعبارات والعناوين المسموح بها والممنوعة، والتي يستخدمها المكون :مكافحة البريد الإلكتروني غير المرغوب فيه"، وقوائم عناوين الويب وأرقام هواتف ISP الموثوقة، وقواعد استثناء الحماية التي تم إنشاؤها لمكونات التطبيق، وقواعد التصفية التي يتم تطبيقها بواسطة "جدار الحماية" على الحزم والتطبيقات.

يتم إنشاء هذه الإعدادات عند العمل مع Kaspersky Total Security فيما يتعلق بالمهام الفردية ومتطلبات الأمان. توصيك Kaspersky Lab بحفظ إعداداتك الخاصة عند استعادة إعدادات التطبيق الافتراضية.

حدد خانات الاختيار الخاصة بالإعدادات التي تريد حفظها، وانقر فوق الزر **التالي**.

الخطوة 3. تحليل نظام التشغيل

يتم في هذه المرحلة البحث عن معلومات حول تطبيقات Microsoft Windows. تتم إضافة هذه التطبيقات إلى قائمة التطبيقات الموثوق بها. لا يتم وضع قيود على الإجراءات التي تنفذها التطبيقات الموثوق بها في نظام التشغيل.

بمجرد اكتمال التحليل، سيتابع "المعالج" تلقائيًا إلى الخطوة التالية.

الخطوة 4. إنهاء الاستعادة

لإغلاق المعالج بعد إتمام مهمته، انقر الزر **إنهاء**.

عرض تقرير تشغيل التطبيق

يحتفظ Kaspersky Total Security بتقارير تشغيل كل مكون من مكونات الحماية. باستخدام تقرير، يمكنك الحصول على معلومات إحصائية حول تشغيل التطبيق (على سبيل المثال، تعرف على كيفية اكتشاف الكثير من الكائنات الضارة وإبطالها لفترة زمنية محددة، وكم عدد مرات تحديث التطبيق لنفس الفترة، وعدد رسائل البريد الإلكتروني غير المرغوب فيها التي تم اكتشافها، وغير ذلك المزيد). يتم الاحتفاظ بالتقارير بتنسيق مشفر.

لعرض تقرير تشغيل التطبيق:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **إظهار الأدوات الإضافية**. سيتم فتح النافذة **أدوات**.
3. في نافذة **الأدوات**، انقر فوق الرابط **التقرير** لفتح نافذة **التقارير**.

   تعرض النافذة **التقارير** تقارير حول تشغيل التطبيق لليوم الحالي (في الجزء الأيمن من النافذة) ولفترة زمنية معينة (في الجزء الأيسر من النافذة).
4. إذا كنت تريد عرض تقرير تفصيلي حول تشغيل التطبيق، ففي الجزء العلوي من نافذة **التقارير** انقر فوق رابط **تقارير تفصيلية**. ومن ثم تفتح نافذة **تقارير تفصيلية**.

تعرض النافذة **تقارير تفصيلية** البيانات في شكل جدول. ولسهولة عرض التقارير، يمكنك تحديد العديد من خيارات الفرز.

تطبيق إعدادات التطبيق على كمبيوتر آخر

بعد تكوين التطبيق، يمكنك تطبيق إعداداته على نسخة Kaspersky Total Security مثبتة على كمبيوتر آخر. ونتيجة لذلك، سيتم تكوين التطبيق بشكل متطابق على جهازي الكمبيوتر.

يتم حفظ إعدادات التطبيق في ملف التكوين الذي يمكنك نقله من كمبيوتر إلى آخر.

يتم نقل إعدادات Kaspersky Total Security من كمبيوتر إلى آخر في ثلاث خطوات:

1. احفظ إعدادات التطبيق في ملف التكوين.
2. انقل ملف التكوين إلى كمبيوتر آخر (مثال، بواسطة البريد الإلكتروني أو على قرص قابل للإزالة).
3. قم باستيراد الإعدادات من ملف التكوين على نسخة التطبيق المثبتة على كمبيوتر آخر.

لتصدير إعدادات التطبيق:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الإعدادات** لفتح نافذة **الإعدادات**.
3. في نافذة **الإعدادات**، حدد القسم **عام**.
4. في القائمة المنسدلة **إدارة الإعدادات** حدد **تصدير الإعدادات**.

   تفتح نافذة **حفظ باسم**.
5. حدد اسمًا لملف التكوين ثم انقر فوق الزر **حفظ**.

تم الآن حفظ إعدادات التطبيق في ملف التكوين.

كما يمكنك تصدير إعدادات التطبيق في موجه الأوامر باستخدام الأمر التالي: avp.com EXPORT <file_name>.

لاستيراد الإعدادات إلى نسخة التطبيق المثبتة على كمبيوتر آخر:

1. على الكمبيوتر الآخر، افتح نافذة التطبيق الرئيسية لـ Kaspersky Total Security.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الإعدادات** لفتح نافذة **الإعدادات**.
3. في نافذة **الإعدادات**، حدد القسم **عام**.
4. في القائمة المنسدلة **إدارة الإعدادات** حدد **استيراد الإعدادات**.

   سيتم فتح نافذة **فتح**.
5. حدد ملف تكوين وانقر فوق الزر **فتح**.

يتم استيراد الإعدادات إلى التطبيق المثبت على الكمبيوتر الآخر.

المشاركة في شبكة اتصال أمان KASPERSKY (KSN)

لحماية الكمبيوتر بشكل أكثر فعالية، يستخدم Kaspersky Total Security البيانات التي تم استلامها من المستخدمين في جميع أنحاء العالم. صُممت شبكة أمان Kaspersky لجمع هذه البيانات.

شبكة أمان Kaspersky (KSN) هي بنية أساسية من خدمات الإنترنت التي توفر إمكانية الوصول إلى قاعدة بيانات Kaspersky Lab، والتي تتضمن معلومات حول سمعة الملفات، وموارد الويب، والبرامج. إن استخدام البيانات من شبكة أمان Kaspersky يضمن الاستجابات بشكل أسرع من قِبل Kaspersky Total Security للتهديدات الجديدة، كما أنه يُحسِّن من أداء بعض مكونات الحماية، ويقلل أيضًا من احتمال حدوث الحالات الإيجابية الزائفة.

تتيح مشاركة المستخدمين في شبكة أمان Kaspersky لشركة Kaspersky Lab جمع المعلومات حول أنواع التهديدات الجديدة ومصادرها على الفور، وتطوير الحلول لإبطالها، وتقليل عدد الحالات الإيجابية الزائفة. تتيح لك المشاركة في شبكة أمان Kaspersky الوصول إلى إحصائيات سمعة التطبيقات ومواقع الويب.

إذا كنت مشاركًا في Kaspersky Security Network، فيمكنك تلقائيًا إرسال معلومات حول تكوين نظام تشغيلك ووقت بدء وانتهاء العمليات في Kaspersky Total Security إلى Kaspersky Lab (انظر القسم "حول توفير البيانات" على صفحة 31).

في هذا القسم

تمكين المشاركة في شبكة اتصال أمان KASPERSKY وتعطيلها

المشاركة اختيارية في شبكة أمان Kaspersky. يمكنك تمكين أو تعطيل استخدام شبكة أمان Kaspersky عند تثبيت Kaspersky Total Security و / أو في أي لحظة بعد تثبيت التطبيق.

تمكين المشاركة في شبكة أمان Kaspersky أو تعطيلها:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **الإعدادات** لفتح نافذة **الإعدادات**.
3. في القسم **إضافي**، حدد القسم الفرعي **ملاحظات**.

   تعرض النافذة تفاصيل شبكة أمان Kaspersky (KSN) وإعدادات المشاركة في شبكة KSN.
4. قم بتمكين المشاركة في شبكة أمان Kaspersky أو تعطيلها باستخدام الزرين **تمكين** / **تعطيل**:
   - إذا كنت تريد المشاركة في شبكة KSN، فانقر فوق الزر **تمكين**.
   - إذا كنت لا تريد المشاركة في شبكة KSN، فانقر فوق الزر **تعطيل**.

فحص الاتصال بشبكة اتصال أمان KASPERSKY

قد يتم فقد الاتصال مع شبكة أمان Kaspersky للأسباب التالية:

- أنت لا تشارك في شبكة اتصال أمان Kaspersky
- الكمبيوتر الخاص بك غير متصل بالإنترنت.
- حالة المفتاح الحالي لا تسمح بالاتصال بشبكة أمان Kaspersky.

> يتم عرض الحالة الحالية للمفتاح في النافذة **الترخيص**.

لفحص الاتصال بشبكة أمان Kaspersky:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة الرئيسية، انقر فوق الرابط **الإعدادات** لفتح نافذة **الإعدادات**.
3. في القسم **إضافي**، حدد القسم الفرعي **ملاحظات**.

تعرض النافذة حالة الاتصال بشبكة أمان Kaspersky.

استخدام التطبيق من موجه الأوامر

يمكنك استخدام Kaspersky Total Security من موجه الأوامر.

تركيب الجُمل في موجه الأوامر:

avp.com <command> [settings]

لعرض تعليمات حول تركيب الجمل في موجه الأوامر، أدخل الأمر التالي:

avp.com [/? | HELP]

يسمح لك هذا الأمر بالحصول على قائمة كاملة بالأوامر المتوفرة لإدارة Kaspersky Total Security من خلال موجه الأوامر.

للحصول على المساعدة حول تركيب الجُمل الخاصة بأمر محدد، يمكنك إدخال واحد من الأوامر التالية:

avp.com <command> /?

avp.com HELP <command>

من موجه الأوامر، يمكنك الرجوع إلى التطبيق إما من مجلد تثبيت التطبيق أو عبر تحديد المسار الكامل إلى avp.com.

الاتصال بالدعم الفني

يوفر هذا القسم معلومات حول كيفية الحصول على الدعم الفني ومتطلبات تلقي التعليمات من الدعم الفني.

في هذا القسم

كيفية الحصول على الدعم الفني

في حالة عدم تمكنك من العثور على حل لمشكلتك في وثائق التطبيق أو في أي من مصادر المعلومات الخاصة بالتطبيق (راجع القسم "مصادر معلومات حول التطبيق" على الصفحة 12)، نوصيك بالاتصال بالدعم الفني لـ Kaspersky Lab. وسوف يجيب أخصائيو الدعم الفني على أي من تساؤلاتك حول تثبيت التطبيق واستخدامه.

قبل الاتصال بالدعم الفني، الرجاء قراءة قواعد الدعم (http://support.kaspersky.com/support/rules).

يمكنك الاتصال بالدعم الفني بإحدى الطرق التالية:

- عبر الهاتف. تتيح لك هذه الطريقة إمكانية استشارة الأخصائيين من الدعم الفني باللغة الروسية أو الدعم الفني العالمي.
- إرسال طلب من منفذ My Kaspersky. تتيح لك هذه الطريقة الاتصال بالمتخصصين لدينا باستخدام نموذج الاستعلام.

يتوفر الدعم الفني فقط للمستخدمين الذين اشتروا ترخيصًا لاستخدام التطبيق. لن يتم توفير الدعم الفني لمستخدمي الإصدارات التجريبية.

الدعم الفني عبر الهاتف

في حالة حدوث مشكلة ملحة، يمكنك الاتصال بالمتخصصين من الدعم الفني باللغة الروسية أو الدعم الفني العالمي عبر الهاتف (http://support.kaspersky.com/support/international) عبر الهاتف.

قبل الاتصال بالدعم الفني، الرجاء قراءة قواعد الدعم (http://support.kaspersky.com/support/rules). فإن هذا سيمكن خبراءنا من تقديم المساعدة بشكل أسرع.

الحصول على الدعم الفني على مدخل My Kaspersky

My Kaspersky هو منطقتك الشخصية (https://my.kaspersky.com) على موقع الويب الخاص بالدعم الفني.

للحصول على حق الوصول إلى مدخل My Kaspersky، يجب التسجيل على صفحة التسجيل (https://my.kaspersky.com/registration). أدخل عنوان البريد الإلكتروني الخاص بك وكلمة مرور لتسجيل الدخول في مدخل My Kaspersky.

يمكنك إجراء ما يلي على مدخل My Kaspersky:

- الاتصال بالدعم الفني ومعمل الفيروسات.
- الاتصال بالدعم الفني دون استخدام البريد الإلكتروني.
- تتبع حالة طلباتك في الحال.
- عرض سجل تفصيلي بطلباتك المتعلقة بالدعم الفني.
- استلام نسخة من ملف المفتاح في حالة فقده أو حذفه.

الدعم الفني باستخدام البريد الإلكتروني

يمكنك إرسال طلب عبر الإنترنت إلى الدعم الفني باللغة الإنجليزية، أو الروسية، أو الألمانية، أو الفرنسية، أو الإسبانية.

في حقول نموذج الطلب عبر الإنترنت، حدد البيانات التالية:

- نوع الطلب
- اسم التطبيق ورقم الإصدار
- وصف الطلب
- مُعرِّف العميل وكلمة المرور
- عنوان البريد الإلكتروني

سيقوم أحد المتخصصين في الدعم الفني بإرسال إجابة إلى طلبك عبر مدخل My Kaspersky وإلى عنوان البريد الإلكتروني الذي حددته في طلبك المقدم عبر الإنترنت.

طلب عبر الإنترنت إلى معمل الفيروسات

يجب إرسال بعض الطلبات إلى معمل الفيروسات بدلاً من الدعم الفني.

يمكنك إرسال الطلبات لفحص الملفات وموارد الويب المشكوك فيها إلى "معمل الفيروسات". يمكنك أيضًا الاتصال بمعمل الفيروسات في حالة إنشاء Kaspersky Total Security لحالات زائفة للملفات وموارد الويب التي لا تعتبرها أنت خطرة.

يمكنك أيضًا إرسال طلبات إلى معمل مكافحة الفيروسات من الصفحة التي تحتوي على نموذج الطلب (http://support.kaspersky.com/virlab/helpdesk.html) بدون التسجيل في مدخل My Kaspersky. من هذه الصفحة، ليس عليك تحديد رمز تفعيل التطبيق.

جمع المعلومات الخاصة بالدعم الفني

بعد أن تقوم بإخطار متخصصي الدعم الفني بالمشكلة، قد يطلبون منك إنشاء تقرير ينبغي أن يتضمن معلومات حول نظام التشغيل الخاص بك وإرساله إلى الدعم الفني. وقد يطلب منك متخصصو الدعم الفني إنشاء ملف تتبع. يسمح لك ملف التتبع بتتبع عملية تنفيذ أوامر التطبيق خطوة بخطوة وتحديد مرحلة من مراحل تشغيل التطبيق التي يحدث فيها الخطأ.

بعد أن يقوم متخصصو الدعم الفني بتحليل البيانات التي قمت بإرسالها، يمكنهم إنشاء برنامج AVZ نصي وإرساله إليك. يسمح لك تشغيل برامج AVZ النصية بتحليل العمليات النشطة للرمز الخبيث وفحص النظام بحثًا عن الرمز الخبيث وتنظيف/حذف الملفات المصابة وإنشاء تقارير حول نتائج عمليات فحص النظام.

لتوفير دعم أفضل للقضايا المتعلقة بوظائف التطبيق، قد يطلب منك أحد خبراء الدعم الفني تغيير إعدادات التطبيق مؤقتًا لأغراض تصحيح أخطاء التطبيق بينما تستمر عمليات التشخيص. للقيام بذلك، ربما تحتاج إلى القيام بالإجراءات التالية:

- تفعيل ميزة جمع المعلومات التشخيصية الممتدة.
- تكوين المكونات الفردية الخاصة بالتطبيق عبر تغيير الإعدادات الخاصة التي لا يمكن الوصول إليها من خلال واجهة المستخدم القياسية.
- إعادة تكوين المساحة التخزينية وإرسال المعلومات التشخيصية التي تم جمعها.
- إعداد مقاطع حركة مرور بيانات الشبكة وحفظ حركة مرور بيانات الشبكة في ملف.

سوف يمنحك خبراء الدعم الفني جميع المعلومات المطلوبة لاتخاذ هذه الإجراءات (اتباع التعليمات خطوة بخطوة، والإعدادات المطلوب تغييرها والبرامج النصية وميزات سطر الأوامر الإضافية ووحدات تصحيح الأخطاء والأدوات الخاصة وما إلى ذلك) وسوف يطلعونك على البيانات التي سوف يتم جمعها لأغراض تصحيح الأخطاء. بعد جمع المعلومات التشخيصية الممتدة، يتم حفظها على كمبيوتر المستخدم. لا يتم إرسال البيانات المجموعة إلى Kaspersky Lab تلقائيًا.

ننصحك بتنفيذ الإجراءات السابقة تحت توجيه خبير الدعم الفني فقط وبعد تلقي تعليمات للقيام بذلك. تغيير إعدادات التطبيق بنفسك على نحو غير الموضح في دليل المسؤول هذا أو على نحو غير موصى به بواسطة خبراء الدعم الفني، قد يتسبب في بطء وتعطل نظام التشغيل، وخفض مستوى حماية الكمبيوتر والفشل في توفير المعلومات المعالجة والحفاظ على سلامتها.

في هذا القسم

إنشاء تقرير حالة النظام

لإنشاء تقرير حالة النظام:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الدعم** لفتح نافذة **الدعم**.
3. في النافذة التي ستفتح، انقر فوق الرابط **أدوات الدعم**.

   سيتم فتح النافذة **أدوات الدعم**.
4. في النافذة التي يتم فتحها، انقر فوق الرابط **إنشاء تقرير حالة النظام**.

يتم إنشاء تقرير حالة النظام بالتنسيقين HTML وXML/ ويتم حفظه في الأرشيف sysinfo.zip. عندما يتم استرداد المعلومات حول نظام التشغيل بالكامل، يمكنك عرض التقرير.

لعرض التقرير، قم بتنفيذ ما يلي:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الدعم** لفتح نافذة **الدعم**.

3. في النافذة التي ستفتح، انقر فوق الرابط **أدوات الدعم**.

سيتم فتح النافذة **أدوات الدعم**.

4. في النافذة التي ستفتح، انقر فوق الارتباط **عرض التقرير**.

سيتم فتح النافذة Microsoft Windows Explorer.

5. في النافذة التي ستفتح، قم بفتح الأرشيف المسمى sysinfo.zip الذي يحتوي على ملفات التقرير.

إرسال ملفات البيانات

بعد إنشاء ملفات التتبع وتقرير حالة النظام، فإنك بحاجة إلى إرسالها إلى خبراء الدعم الفني في Kaspersky Lab.

وسوف تكون بحاجة إلى رقم طلب لرفع ملفات إلى خادم الدعم الفني. يتوفر هذا الرقم على مدخل My Kaspersky عندما يكون لديك طلب نشط.

لتحميل ملفات البيانات إلى خادم الدعم الفني:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الدعم** لفتح نافذة **الدعم**.
3. في النافذة التي ستفتح، انقر فوق الرابط **أدوات الدعم**.

   سيتم فتح النافذة **أدوات الدعم**.
4. في النافذة التي سيتم فتحها، انقر فوق الرابط **إرسال تقرير إلى الدعم الفني**.

   ومن ثم تفتح نافذة **إرسال تقرير**.
5. حدد خانات الاختيار بجوار البيانات التي تريد إرسالها إلى الدعم الفني.
6. انقر فوق الزر **إرسال التقرير**.

يتم حزم ملفات التتبع المحددة وإرسالها إلى خادم الدعم الفني.

إذا كان من غير الممكن لأي سبب من الأسباب الاتصال بالدعم الفني، فيمكن تخزين ملفات البيانات على جهاز الكمبيوتر وإرساله فيما بعد من مدخل My Kaspersky.

لحفظ ملفات البيانات على القرص:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الدعم** لفتح نافذة **الدعم**.
3. في النافذة التي ستفتح، انقر فوق الرابط **أدوات الدعم**.
4. سيتم فتح النافذة **أدوات الدعم**.
5. في النافذة التي سيتم فتحها، انقر فوق الرابط **إرسال تقرير إلى الدعم الفني**.

   ومن ثم تفتح نافذة **إرسال تقرير**.
6. حدد أنواع البيانات التي تريد إرسالها:

- **معلومات النظام**. حدد خانة الاختيار هذه لإرسال معلومات حول نظام التشغيل على الكمبيوتر إلى الدعم الفني.
- **البيانات المجمعة للتحليل**. حدد خانة الاختيار هذه لإرسال ملفات تتبع التطبيق إلى الدعم الفني. انقر فوق الرابط <**عدد الملفات**>، <**حجم البيانات**> لفتح النافذة **البيانات المجمعة للتحليل**. حدد خانات الاختيار المقابلة لملفات التتبع التي تريد إرسالها.

7. انقر فوق الرابط **حفظ التقرير**.

   يتم فتح نافذة لحفظ الأرشيف.

8. حدد اسم الأرشيف ثم أكد الحفظ.

يمكن إرسال الأرشيف الذي تم إنشاؤه إلى الدعم الفني من مدخل My Kaspersky.

المحتويات ومخزن ملفات التتبع

يتم تخزين ملفات التتبع على الكمبيوتر في نموذج مشفر طالما أن التطبيق قيد الاستخدام، ويتم حذفها نهائيًا عند إزالة التطبيق.

يتم تخزين ملفات التتبع في مجلد ProgramData\Kaspersky Lab.

تنسيق أسماء ملف التتبع هو كما يلي: KAV<version number_dataXX.XX_timeXX.XX_pidXXX.><trace file type>.log.enc1.

تحتوي جميع ملفات التتبع على البيانات الشائعة التالية:

- وقت الحدث.
- عدد ترابط التنفيذ.
- مكون التطبيق الذي أدى إلى الحدث.
- درجة خطورة الحدث (حدث معلوماتي وتحذير وحدث حرج وخطأ).
- وصف الحدث الذي يتضمن تنفيذ الأمر بواسطة مكون التطبيق ونتيجة تنفيذ هذا الأمر.

محتويات ملفات التتبع **SRV.log** و**GUI.log** و**ALL.log**

قد تقوم ملفات التتبع SRV.log وGUI.log بتخزين المعلومات التالية:

- البيانات الشخصية، بما في ذلك اسم العائلة والاسم الأول واسم العائلة المركب، إذا تم تضمين هذه البيانات في المسار المؤدي إلى الملفات على كمبيوتر محلي.
- اسم المستخدم وكلمة المرور إذا تم إرسالهما على نحو مفتوح. يمكن تسجيل هذه البيانات في ملفات التتبع أثناء فحص حركة مرور الإنترنت. يتم تسجيل حركة المرور في ملفات التتبع فقط من trafmon2.ppl.
- يتم تضمين اسم المستخدم وكلمة المرور في رؤوس HTTP.
- اسم حساب Microsoft Windows إذا تم تضمين اسم الحساب في اسم ملف.
- عنوان البريد الإلكتروني أو عنوان الويب الذي يحتوي على اسم حسابك وكلمة المرور إذا تم تضمينهما في اسم الكائن الذي تم اكتشافه.

- مواقع الويب الذي قمت بزيارتها أو إعادة التوجيه من مواقع الويب هذه. تتم كتابة هذه البيانات لملفات التتبع عندما يقوم التطبيق بفحص مواقع الويب.
- عنوان خادم الوكيل واسم الكمبيوتر والمنفذ وعنوان IP واسم المستخدم المخصص لتسجيل الدخول إلى خادم الوكيل. تتم كتابة هذه البيانات إلى ملفات التتبع إذا كان التطبيق يستخدم خادم وكيل.
- عناوين IP عن بُعد التي قام الكمبيوتر بإنشاء اتصالات لها.
- عنوان الرسالة والمعرف واسم المرسل وعنوان صفحة ويب مرسل الرسالة على شبكة اجتماعية. تتم كتابة هذه البيانات إلى ملفات التتبع إذا تم تمكين مكون الرقابة الأسرية.

محتويات ملفات التتبع **HST.log** و **BL.log** و **Dumpwriter.log**

يحتوي ملف التتبع HST على معلومات حول مهمة تحديث تنفيذ قاعدة بيانات ووحدة التطبيق.

يحتوي ملف التتبع BL على معلومات حول الأحداث التي حدثت أثناء تشغيل التطبيق بالإضافة إلى البيانات المطلوبة لاكتشاف أخطاء التطبيق وإصلاحها. يتم إنشاء هذا الملف في حالة بدء التطبيق بمعلمة avp.exe –bl.

يحتوي ملف التتبع dumpwriter.log على معلومات الخدمة المطلوبة لاكتشاف الأخطاء التي تحدث عند كتابة تفريغ ذاكرة التطبيق.

محتويات ملفات تتبع مكونات التطبيق الإضافية

تحتوي ملفات تتبع مكونات التطبيق الإضافية على المعلومات التالية:

- يحتوي VirtualKeyboard (VKB.log) على معلومات الخدمة حول تشغيل المكون الإضافي والبيانات المطلوبة لاستكشاف أخطاء المكون الإضافي وإصلاحها.
- تحتوي العمليات البنكية عبر الإنترنت (OB.log) على معلومات الخدمة حول عملية تشغيل المكون الإضافي، بما في ذلك معلومات حول أحداث فحص موقع الويب ونتائج الفحص والاتصالات بعناوين IP وإعدادات الخادم الوكيل وملفات تعريف الارتباط. يحتوي الملف أيضًا على البيانات المطلوبة لاستكشاف أخطاء المكون الإضافي وإصلاحها.
- يحتوي ContentBlocker (CB.log) على معلومات الخدمة حول عملية تشغيل المكون الإضافي، بما في ذلك معلومات حول أحداث فحص موقع الويب ونتائج الفحص والاتصالات بعناوين IP وإعدادات الخادم الوكيل. يحتوي الملف أيضًا على البيانات المطلوبة لاستكشاف أخطاء المكون الإضافي وإصلاحها.
- يحتوي مكون مكافحة فيروسات المكتب (OA.log) على معلومات حول فحص مستندات Microsoft Office. قد يحتوي هذا الملف أيضًا على معلومات حول المسار الكامل إلى مستند أو عنوان موقع ويب تم تنزيل هذا المستند منه.
- يبدأ ملف تتبع المكون الإضافي مهمة فحص من قائمة سياقية (shellex.dll.log). تحتوي على معلومات حول تنفيذ مهمة فحص والبيانات المطلوبة لاستكشاف أخطاء المكون الإضافي وإصلاحها.
- ملفات تتبع المكون الإضافي Microsoft Outlook:
  - mcouas.OUTLOOK.EXE. المكون الإضافي لمكافحة البريد الإلكتروني غير المرغوب فيه
  - mcou.OUTLOOK.EXE. المكون الإضافي لمكافحة فيروسات البريد

  يمكن أن تحتوي الملفات على أجزاء من رسائل البريد الإلكتروني، بما في ذلك العناوين.
- ملف التتبع الخاص بالمكون الإضافي لتسجيل امتداد Google Chrome (NativeMessagingHost.log). يحتوي على معلومات الخدمة حول عملية تشغيل المكون الإضافي.

تشغيل نصوص AVZ

ننصح بعدم تغيير نص البرنامج النصي AVZ الذي استلمته من خبراء Kaspersky Lab. عند حدوث مشكلات أثناء تنفيذ البرنامج النصي، الرجاء الاتصال بالدعم الفني.

لتشغيل برنامج AVZ النصي:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر فوق الرابط **الدعم** لفتح نافذة **الدعم**.
3. في النافذة التي ستفتح، انقر فوق الرابط **أدوات الدعم**.

   سيتم فتح النافذة **أدوات الدعم**.
4. في النافذة التي يتم فتحها، انقر فوق الرابط **تشغيل البرنامج النصي**.

   يتم فتح نافذة **تشغيل البرنامج النصي**.
5. انسخ النص من البرنامج النصي المرسل بواسطة المتخصصين في الدعم الفني، وألصقه في حقل الإدخال في النافذة التي ستفتح وانقر فوق الزر **تشغيل**.

يتم تشغيل البرنامج النصي.

في حالة نجاح تنفيذ البرنامج النصي، يتم إغلاق المعالج. في حالة حدوث خطأ خلال تنفيذ البرنامج النصي، يعرض المعالج رسالة معنية.

القيود والتحذيرات

ينطوي Kaspersky Total Security على عدد من القيود غير المهمة لتشغيل التطبيق.

قيود حول الترقيات من إصدار سابق للتطبيق

- أثناء ترقية إصدار سابق من Kaspersky Total Security، تتم إعادة ضبط إعدادات التطبيق التالية على قيمها الافتراضية: مصادر التحديث، وقائمة عناوين مواقع الويب الموثوق بها، وإعدادات "مستشار Kaspersky لعناوين مواقع الويب".
- عند تثبيت إصدار جديد لـ Kaspersky Total Security على إصدار Kaspersky PURE أقل من 2.0، يتم فقدان ملفات النسخ الاحتياطي والكائنات المعزولة نظرًا لأن تنسيقها غير مدعوم ولا يمكن تحويله إلى التنسيق الجديد. أثناء الترقية من Kaspersky PURE الإصدار 2.0، يمكن تحويل نُسخ الملفات الاحتياطية والكائنات المعزولة إلى التنسيق الجديد. يُعد تنسيق مخزن النسخ الاحتياطي في Kaspersky PURE 3.0 مدعوم ولا يتطلب التحويل إلى التنسيق الجديد.

قيود حول تشغيل مكونات معينة والمعالجة التلقائية للملفات

تتم معالجة الملفات المصابة تلقائيًا وفقًا للقواعد التي تم إنشاؤها بواسطة متخصصي Kaspersky Lab. لا يمكنك تعديل هذه القواعد يدويًا. يمكن تحديث القواعد بعد تحديث قواعد البيانات ووحدات التطبيق النمطية. يتم أيضًا تحديث قواعد وضع جدار الحماية والتحكم في التطبيق والتطبيقات الموثوقة تلقائيًا.

فحص شهادة موقع الويب وقيود فحص الملف

عند فحص شهادة موقع ويب أو فحص ملفات موقع ويب، قد يتصل التطبيق بـ Kaspersky Security Network للحصول على معلومات. إذا تعذر استرداد البيانات من Kaspersky Security Network، فيقرر التطبيق ما إذا كان الملف مصاب أم لا وعدم الوثوق في الشهادة بناءً على قواعد بيانات مكافحة الفيروسات المحلية.

قيود وظائف مكون مراقب النظام

تحتوي وظائف نُسخ الملفات الاحتياطية التي تم تشفيرها بواسطة أداة تشفير خبيثة على القيود التالية:

- إذا لم تكن هناك مساحة كافية على قرص النظام بحيث يوجد عليه مجلد Temp، فلا يمكن إجراء أي نسخ احتياطي، ولا يتم عرض أي إخطارات بوجود نسخ فاشل (حماية غير متوفرة).
- يمكن حفظ النسخ الاحتياطية للملفات بتنسيق غير مشفر.
- يتم حذف نسخ الملفات الاحتياطية عند غلق Kaspersky Total Security أو تعطيل مكون مراقب النظام.
- في حالة الإنهاء الطارئ لـ Kaspersky Total Security، لا يتم حذف النسخ الاحتياطية. وفي هذه الحالة، يجب عليك حذفها يدويًا.

تحذير حول المعلومات التشخيصية التي تم تجميعها

يتم تشفير المعلومات التشخيصية حول تشغيل التطبيق، الذي تقوم بتجميعها من أجل الدعم الفني، أثناء تجميعها. وإذا لزم الأمر، يمكنك تعطيل التشفير.

قيود وظائف الاتصالات الآمنة

نظرًا للقيود الفنية لتنفيذ خوارزميات الفحص، لا يدعم فحص الاتصالات الآمنة امتدادات معينة لبروتوكول TLS 1.0 والإصدارات الأحدث (خصوصًا NPN وALPN). قد تكون الاتصالات عبر هذه البروتوكولات مقيدة. تستخدم مستعرضات الويب التي تدعم

بروتوكول SPDY بروتوكول HTTP فوق TLS بدلاً من بروتوكول SPDY حتى لو كان الخادم الذي تم تعيين الاتصال عليه يدعم SPDY. وهذا لا يؤثر على مستوى أمان الاتصال.

تحذير حول تشغيل مكون مكافحة البريد الإلكتروني غير المرغوب فيه

يمكن تكوين وظائف مكافحة البريد الإلكتروني غير المرغوب فيه عن طريق تحرير ملف إعدادات مكون مكافحة البريد الإلكتروني غير المرغوب فيه.

قيود النسخ الاحتياطي

يتم تطبيق القيود التالية على النسخ الاحتياطي:

- لا يتوفر التخزين عبر الإنترنت للنسخ الاحتياطية عند استبدال محرك الأقراص الثابتة أو الكمبيوتر. قم بزيارة موقع ويب دعم Kaspersky Lab للحصول على معلومات حول كيفية استعادة الاتصال بالمخزن عبر الإنترنت بعد استبدال الأجهزة.
- قد يؤدي تحرير ملفات خدمة مخزن النسخ الاحتياطي إلى فقدان الوصول إلى مخزن النسخ الاحتياطي وعدم القدرة على استعادة بياناتك.

قيود وظائف تشفير البيانات

عند إنشاء مخزن بيانات في ملف النظام FAT32، يجب ألا يتجاوز حجم ملف مخزن البيانات على محرك الأقراص 4 جيجا بايت.

مواصفات فحص ذاكرة النواة للتعرف على الفيروسات الجذرية في وضع المستعرض المحمي

عند اكتشاف وحدة نمطية غير موثوق بها في وضع المستعرض المحمي، يتم فتح علامة تبويب مستعرض جديدة مع إخطار باكتشاف برامج ضارة. إذا حدث ذلك، فإننا نوصي بالخروج من المستعرض وتشغيل الفحص الكامل للكمبيوتر.

مواصفات حماية بيانات الحافظة

يسمح Kaspersky Total Security للتطبيق بالوصول إلى الحافظة في الحالات التالية:

- محاولة تطبيق ذو نافذة نشطة وضع البيانات في الحافظة. النافذة النشطة هي النافذة التي تستخدمها حاليًا.
- محاولة عملية موثوقة لتطبيق وضع بيانات في الحافظة.
- محاولة عملية موثوقة لتطبيق أو عملية ذات نافذة نشطة تلقي بيانات من الحافظة.
- محاولة عملية تطبيق قامت بوضع بيانات في الحافظة سابقًا تلقي هذه البيانات من الحافظة.
- عند إنهاء العملية النشطة للمستعرض المحمي، يقوم Kaspersky Total Security بمسح الحافظة، ما لم يتم إجراء عملية الحافظة الأخيرة بواسطة عملية موثوقة.

تحذير حول التوافق مع تطبيقات **Kaspersky Lab**

يتوافق Kaspersky Total Security مع تطبيقات Kaspersky Lab التالية:

- Kaspersky Fraud Prevention 2.5
- Kaspersky Fraud Prevention 3.0
- Kaspersky Password Manager 2.0
- Kaspersky Password Manager 5.0
- Kaspersky Password Manager 7.0

المصطلحات

HYPERVISOR

رمز البرنامج الخاص بإدارة العملية الظاهرية.

ROOTKIT

برنامج أو مجموعة من البرامج لإخفاء تتبع مهاجم أو برنامج ضار في نظام التشغيل.

في أنظمة التشغيل التي تعتمد على Windows، يشير فيروس الجذر عادة إلى برنامج يخترق نظام التشغيل ويقاطع وظائف النظام (Windows API). يُعد اعتراض وتعديل وظائف API ذات المستوى المنخفض هي الطرق الرئيسية التي تتيح لمثل هذا البرنامج بالتواجد في نظام التشغيل بشكل متخفٍ تمامًا. بإمكان فيروس الجذر في الغالب أيضًا أن يخفي وجود عمليات ومجلدات وملفات مخزنة على محرك أقراص، بالإضافة إلى مفاتيح التسجيل، وذلك إذا ما تم وصف هذه الأشياء في تكوين فيروس الجذر. والعديد من فيروسات الجذور تقوم بتثبيت برامج تشغيل وخدمات خاصة بها هي على نظام التشغيل (حيث تكون هذه الخدمات أيضًا "غير مرئية").

تقنية iChecker

تقنية تسمح بزيارة سرعة عمليات الفحص لمكافحة الفيروسات من خلال استثناء الكائنات التي لم تتغير منذ آخر مرة تم فحصها، بشرط عدم تعديل معلمات الفحص (قواعد البيانات والإعدادات). ويتم تخزين المعلومات الخاصة بكل ملف في قاعدة بيانات خاصة. ويتم استخدام هذه التقنية في أوضاع الحماية الفورية والفحص عند الطلب.

على سبيل المثال، لديك ملف أرشيف تم فحصه بواسطة تطبيق Kaspersky Lab وتخصيص الحالة غير مصاب له. في المرة القادمة سيقوم التطبيق بتخطي هذا الأرشيف ما لم يتم تنبيه التطبيق أو ما لم يتم تغيير إعدادات الفحص. وإذا قمت بتغيير محتوى الأرشيف بإضافة كائن جديد إليه، أو تعديل إعدادات الفحص، أو تحديث قواعد بيانات التطبيق، ستتم إعادة فحص الأرشيف.

حدود تقنية iChecker:

لا تعمل هذه التقنية مع الملفات الكبيرة، حيث إنه من الأسرع فحص الملف بدلاً من التحقق مما إذا كان قد تم تعديله منذ آخر عملية فحص.

تدعم التقنية عددًا محدودًا من التنسيقات.

تطبيق غير متوافق

تطبيق مكافحة فيروسات من تطوير طرف ثالث أو أن تطبيق Kaspersky Lab لا يدعم الإدارة عبر Kaspersky Total Security.

كائن مصاب

كائن يتطابق جزءُ من رمزه تمامًا مع جزء من برنامج خبيث غير معروف. لا توصي Kaspersky Lab بالوصول إلى مثل هذه الكائنات.

خوادم تحديث Kaspersky Lab

خوادم Kaspersky Lab HTTP التي يتم منها تنزيل تحديثات قواعد البيانات والوحدات البرمجية.

شبكة اتصال أمان Kaspersky (KSN)

بنية أساسية من خدمات الإنترنت التي توفر إمكانية الوصول إلى قاعدة بيانات Kaspersky Lab، والتي تتضمن معلومات حول سمعة الملفات، وموارد الويب، والبرامج. إن استخدام البيانات من شبكة أمان Kaspersky يضمن الاستجابات بشكل أسرع من قِبل تطبيقات Kaspersky Lab للتهديدات الجديدة، كما أنه يُحسِّن من أداء بعض مكونات الحماية، ويقلل أيضًا من مخاطر الحالات الإيجابية الزائفة.

راصد لوحة المفاتيح

هو برنامج مصمم لتسجيل معلومات حول المفاتيح التي يضغط عليها المستخدم بشكل غير ظاهر. تعمل برامج رصد لوحة المفاتيح كبرامج اعتراض لضغطات لوحة المفاتيح.

فترة الترخيص

هي الفترة الزمنية التي يمكنك خلالها الوصول إلى مزايا التطبيق وحقوق استخدام الخدمات الإضافية.

الاحتيال

نوع من الاحتيال على الإنترنت يهدف إلى الحصول على إمكانية وصول غير مصرح بها لبيانات المستخدم السرية.

بريد إلكتروني يُحتمل أن يكون غير مرغوب فيه

هي رسالة لا يمكن اعتبارها دون شك بريدًا إلكترونيًا غير مرغوب فيه، لكنها تشتمل على سمات عديدة من سمات البريد الإلكتروني غير المرغوب فيه (على سبيل المثال، بعض أنواع المراسلات والرسائل الإعلانية).

كائن يحتمل كونه مصابًا

كائن يحتوي الرمز الخاص به على رمز معدل من تهديد معروف، أو كائن سلوكه مماثل لكائن يمثل تهديدًا.

المستعرض المحمي

وضع تشغيل مخصص لمستعرض ويب قياسي مصمم للأنشطة المالية والتسوق عبر الإنترنت. يضمن استخدام المستعرض المحمي سلامة البيانات السرية التي قمت بإدخالها على مواقع ويب البنوك وأنظمة السداد (مثل أرقام البطاقات البنكية أو كلمات المرور الخاصة بالوصول إلى الخدمات البنكية عبر الإنترنت)؛ كما يمنع أيضًا سرقة الأصول عند نقل الأموال عبر الإنترنت. في نفس الوقت، يعرض المستعرض القياسي المستخدم للوصول إلى موقع الويب رسالة تخبرك بتشغيل المستعرض المحمي.

مكونات الحماية

هي أجزاء لا تتجزأ من Kaspersky Total Security مخصصة لضمان الحماية ضد أنواع معينة من التهديدات (مثل "مكافحة البريد الإلكتروني غير المرغوب فيه" و"مكافحة الاحتيال"). يتميز كل مكون من هذه المكونات بأنه مستقل نسبيًا عن المكونات الأخرى، ولذلك يمكن تعطيله أو تكوينه على حدة.

البروتوكول

مجموعة من القواعد القياسية المعرفة بوضوح التي تنظم التعامل بين أي عميل وأي خادم. تتضمن البروتوكولات المعروفة والخدمات المصاحبة لها HTTP، وFTP، وNNTP.

العزل

مخزن مخصص يضع فيه التطبيق نُسخًا احتياطية من الملفات التي تم تعديلها أو حذفها أثناء عملية التنظيف. يتم تخزين نُسخ الملفات بتنسيق خاص لا يمثل خطورة على الكمبيوتر.

البرنامج النصي

برنامج كمبيوتر صغير أو جزء مستقل من برنامج (وظيفة)، والذي يتم تطويره، كقاعدة، لتنفيذ مهمة معينة. ويستخدم غالباً مع البرامج المضمنة في النص التشعبي. وتعمل البرامج النصية عند فتح بعض مواقع ويب معينة على سبيل المثال.

إذا تم تمكين الحماية في الوقت الحقيقي، فيقوم التطبيق بتتبع تنفيذ البرامج النصية واعتراضها وفحصها للبحث عن الفيروسات. ووفقاً لنتائج الفحص، يمكنك منع تنفيذ برنامج نصي أو السماح بذلك.

مستوى الأمان

يتم تعريف مستوى الأمان كمجموعة سابقة التحديد من الإعدادات لأحد مكونات التطبيقات.

البريد الإلكتروني غير المرغوب فيه

غالباً ما تحتوي كميات ضخمة من رسائل البريد الإلكتروني غير المرغوب فيها على رسائل دعائية.

كائنات بدء التشغيل

مجموعة البرامج اللازمة لبدء نظام التشغيل والبرامج المثبتة على جهاز الكمبيوتر وعملها بصورة صحيحة. يتم تنفيذ هذه الكائنات في كل مرة يبدأ فيها نظام التشغيل. هناك فيروسات قادرة على إصابة كائنات التشغيل التلقائي على وجه الخصوص، الأمر الذي قد يؤدي مثلاً إلى منع بدء نظام التشغيل.

المهمة

يتم تنفيذ الوظائف التي تم إجراؤها بواسطة تطبيق Kaspersky Lab كمهام، مثل حماية الملفات في الوقت الفعلي والفحص الكامل للكمبيوتر وتحديث قاعدة البيانات.

إعدادات المهام

هي إعدادات التطبيق الخاصة بكل نوع من أنواع المهام.

مستوى التهديد

هو فهرس يعرض احتمالية تمثيل أحد التطبيقات تهديدًا لنظام التشغيل. يتم حساب مستوى التهديد باستخدام التحليل المساعد على الاكتشاف وفقًا لنوعين من المعايير:

ثابت (مثل معلومات حول الملف التنفيذي لتطبيق: الحجم، وتاريخ الإنشاء، إلخ.)؛

ديناميكي، يتم الاستخدام أثناء تحفيز تشغيل التطبيق في بيئة ظاهرية (تحليل طلبات نظام التطبيق)

يسمح مستوى التهديد باكتشاف أي سلوك مطابق للبرمجيات الخبيثة. كلما انخفض مستوى التهديد، زادت الإجراءات التي سيُسمح للتطبيق القيام بها في نظام التشغيل.

التتبعات

أثناء تشغيل التطبيق في وضع التصحيح؛ بعد تنفيذ كل أمر، يتم إيقاف التطبيق، ويتم عرض نتيجة هذه الخطوة.

فحص حركة البيانات

هو فحص فوري يستخدم معلومات من الإصدار الحالي (أحدث إصدار) من قواعد البيانات للكائنات المنقولة عبر جميع البروتوكولات (مثل HTTP، وFTP والبروتوكولات الأخرى).

مجموعة الثقة

هي مجموعة يخصص فيها Kaspersky Total Security أحد التطبيقات أو إحدى العلميات حسب المعايير التالية: وجود توقيع رقمي، والسمعة في شبكة KSN، ومستوى الثقة بمصدر التطبيق، والخطر المحتمل من الإجراءات التي يقوم بها التطبيق أو العملية. حسب مجموعة الثقة التي ينتمي لها التطبيق، قد يقيد Kaspersky Total Security الإجراءات التي قد ينفذها هذا التطبيق في نظام التشغيل.

في Kaspersky Total Security، تنتمي التطبيقات إلى إحدى مجموعات الثقة التالية: "موثوق، أو "مستوى التقييد منخفض"، أو "مستوى التقييد مرتفع"، أو "غير موثوق".

عملية موثوق بها

هي إحدى عمليات البرنامج التي لا يتم تقييد عمليات الملف الخاص بها بواسطة تطبيق Kaspersky Lab في وضع الحماية في الوقت الفعلي. عند اكتشاف نشاط مشكوك فيه في عملية موثوق بها، يقوم Kaspersky Total Security بإزالة العملية من قائمة العمليات الموثوق بها ويمنع كل إجراءاته.

فيروس غير معروف

هو فيروس جديد لا توجد عنه أية معلومات في قواعد البيانات. وبشكل عام، يتم اكتشاف الفيروسات غير المعروفة بواسطة التطبيق في الكائنات بواسطة استخدام المحلل المساعد على الاكتشاف. ويتم تصنيف هذه الكائنات حسب الإصابة المحتملة.

التحديث

إجراء استبدال/إضافة ملفات جديدة (قواعد بيانات أو وحدات تطبيق) تم استردادها من خوادم تحديث Kaspersky Lab.

حزمة التحديث

حزمة ملف مصممة لتحديث قواعد البيانات والوحدات النمطية للتطبيق. يقوم تطبيق Kaspersky Lab بنسخ حزم التحديث من خوادم تحديث Kaspersky Lab وتثبيتها وتطبيقها بشكل تلقائي.

ملف بيانات المستخدم

ملخص لمشاركة المستخدم في برنامج "حماية الأصدقاء". يشتمل ملف بيانات المستخدم على وعدد نقاط الربح المجمعة، وروابط إلى صفحة تنزيل Kaspersky Total Security، ورموز التفعيل الربحية الممنوحة للمستخدم.

فيروس

هو برنامج يصيب برامج أخرى من خلال إضافة تعليماته البرمجية إليها لاكتساب التحكم عند تشغيل الملفات المصابة. ويوضح هذا التعريف البسيط الإجراء الرئيسي الذي يقوم به أي فيروس: الإصابة.

قابلية الاختراق

خلل في نظام تشغيل أو تطبيق يمكن استغلاله بواسطة مطوري البرمجيات الضارة لاختراق نظام التشغيل أو التطبيق وإتلاف سلامته. إن وجود عدد كبير من الثغرات الأمنية في نظام التشغيل يجعله غير موثوق به نظرًا لأن الفيروسات التي تخترقه قد تسبب فشل تشغيل نظام التشغيل نفسه والتطبيقات المُثبَّتة عليه.

KASPERSKY LAB ZAO

تحظى برامج Kaspersky Lab بشهرة عالمية كبيرة لحمايتها ضد الفيروسات، والبرمجيات الخبيثة، والبريد الإلكتروني غير المرغوب فيه، وهجمات الشبكة والمتسللين، والتهديدات الأخرى.

في عام 2008، تم تصنيف Kaspersky Lab بين أعلى أربعة موردين على مستوى العالم متخصصين في توريد حلول برامج أمان المعلومات للمستخدمين النهائيين (IDC Worldwide Endpoint Security Revenue by Vendor). كما تعتبر Kaspersky Lab من المطورين المفضلين لأنظمة حماية الكمبيوتر بين المستخدمين في المنازل في روسيا، وذلك وفق استطلاع COMCON "TGI-Russia 2009".

تم تأسيس Kaspersky Lab في روسيا في عام 1997. وتتكون اليوم من مجموعة عالمية من الشركات التي اتخذت من موسكو مقرًا لها وتتألف من خمسة فروع إقليمية تقوم بإدارة عمليات الشركة في روسيا، وأوروبا الشرقية والغربية، والشرق الأوسط، وإفريقيا، وأمريكا الشمالية والجنوبية، واليابان والصين والدول الأخرى في منطقة المحيط الهادي الأسيوية. ويعمل تحت إمرتها أكثر من 2،000 موظف من المتخصصين المؤهلين.

المنتجات. توفر منتجات Kaspersky Lab الحماية لجميع الأنظمة - من أجهزة الكمبيوتر المنزلية إلى شبكات الشركات الكبيرة.

ويتضمن نطاق المنتجات الشخصي برنامج مكافحة الفيروسات لجميع الأجهزة المستخدمة في الحياة الرقمية اليوم، حيث يغطي أجهزة كمبيوتر سطح المكتب والمحمولة والهواتف الذكية والأجهزة المحمولة الأخرى.

ويوفر Kaspersky Lab تطبيقات وخدمات لحماية محطات العمل والملفات وخوادم الويب وعبارات البريد وجدران الحماية. وعن طريق الاستخدام المشترك مع نظام الإدارة المركزية لـ Kaspersky Lab، فإن هذه الحلول تضمن وجود حماية فعالة تلقائية للشركات والمنظمات ضد التهديدات الموجهة لأجهزة الكمبيوتر. وقد تم اعتماد منتجات Kaspersky Lab بواسطة كبرى معامل الاختبار وتتوافق مع البرامج الخاصة بمختلف الموردين كما تم تحسينها ليتم تشغيلها على الكثير من الأنظمة الأساسية للأجهزة.

ويعمل محللو الفيروسات في Kaspersky Lab على مدار الساعة. حيث يعثرون كل يوم على المئات من التهديدات الجديدة الموجهة لأجهزة الكمبيوتر، ويقومون بإنشاء أدوات لاكتشافها وتنظيفها، وإضافتها إلى قواعد البيانات التي تستخدمها تطبيقات Kaspersky Lab. *يتم تحديث قاعدة بيانات Kaspersky Lab لمكافحة الفيروسات كل ساعة* وقاعدة *بيانات مكافحة البريد الإلكتروني غير المرغوب فيه كل خمس دقائق.*

التقنيات. لقد تم تطوير العديد من التقنيات التي تعد الآن جزءا لا يتجزأ من أدوات مكافحة الفيروسات الحديثة من قبل Kaspersky Lab. وهذا هو أحد الأسباب في اختيار العديد من مطوري البرامج الخارجيين استخدام محرك Kaspersky Anti-Virus في تطبيقاتهم. ومن بين هذه الشركات Safenet (الولايات المتحدة الأمريكية)، وAlt-N Technologies (الولايات المتحدة الأمريكية)، و Blue Coat Systems (الولايات المتحدة الأمريكية)، Check Point Software Technologies (إسرائيل)، Clearswift (المملكة المتحدة)، وCommunigate Systems (الولايات المتحدة الأمريكية)، وOpenwave Messaging (أيرلندا)، وD-Link (تايوان)، M86 Security (الولايات المتحدة الأمريكية)، وGFI Software (مالطا)، وIBM (الولايات المتحدة الأمريكية)، Juniper Networks (الولايات المتحدة الأمريكية)، LANDesk (الولايات المتحدة الأمريكية)، Microsoft (الولايات المتحدة الأمريكية)، وNETASQ (فرنسا)، NETGEAR (الولايات المتحدة الأمريكية)، Parallels (الولايات المتحدة الأمريكية)، وSonicWALL (الولايات المتحدة الأمريكية)، WatchGuard Technologies (الولايات المتحدة الأمريكية)، ZyXEL Communications (تايوان). ولقد تم الحصول على براءات اختراع للكثير من التقنيات التي ابتكرتها الشركة.

الإنجازات. عبر سنوات طويلة، فازت شركة Kaspersky Lab بمئات الجوائز نظير خدماتها في مكافحة تهديدات الكمبيوتر. على سبيل المثال، ففي عام 2010 فازت Kaspersky لمكافحة الفيروسات بالعديد من الجوائز المتقدمة في اختبار تم تحت إشراف AV-Comparatives، وهو معمل شهير معتمد في النمسا متخصص في مكافحة الفيروسات. ولكن يتمثل الإنجاز الرئيسي لشركة Kaspersky Lab في ولاء مستخدميه في جميع أنحاء العالم. حيث تحمي منتجات وتقنيات الشركة أكثر من 300 مليون مستخدم، ويزيد عدد عملاء الشركة عن 200000 عميل.

موقع ويب Kaspersky Lab:	http://www.kaspersky.com
موسوعة الفيروسات:	http://www.securelist.com
Virus Lab:	newvirus@kaspersky.com (فقط لإرسال الملفات محتملة الإصابة بتنسيق الأرشيف)
منتدى ويب Kaspersky Lab:	http://forum.kaspersky.com

معلومات حول التعليمات البرمجية الخاصة بطرف ثالث

يتم تضمين معلومات حول رمز الطرف الخارجي في ملف باسم legal_notices.txt في مجلد تثبيت التطبيق.

إشعارات العلامة التجارية

العلامات التجارية المسجلة وعلامات الخدمة مملوكة لأصحابها.

Dropbox هي علامة تجارية لـ Dropbox، Inc.

Google وGoogle Chrome وYouTube هي علامات تجارية لـ Google، Inc.

تعتبر Intel وCeleron وAtom وPentium علامات تجارية لشركة Intel Corporation في الولايات المتحدة. و/أو دول أخرى.

يُعد Internet Explorer وMicrosoft وWindows وDirectX وBing وOutlook وWindows Vista علامات تجارية مسجلة لشركة Microsoft Corporation في الولايات المتحدة ودول أخرى.

يعتبر كل من Mozilla وFirefox علامات تجارية لشركة Mozilla.

OpenGL هي علامة تجارية مسجلة لـ SGI.

تُعد VMware علامة تجارية مسجلة أو علامة تجارية لشركة VMware، Inc. في الولايات المتحدة وفي أماكن ذات سلطات قضائية أخرى.

Mail.ru هي علامة تجارية مملوكة لشركة Mail.ru LLC.

فهرس

K

ا

إ

ا

و


KASPERSKY lab